

System and apparatus for smart card personalization

Publication number: JP2000508794T

Publication date: 2000-07-11

Inventor:

Applicant:

Classification:






- international: **G06K17/00; G07F7/10; G06K17/00; G07F7/10;** (IPC1-7): G06K17/00

- European: G07F7/10D2

Application number: JP19970537290T 19970414

Priority number(s): WO1997US06204 19970414; US19960015743P 19960415; US19960755459 19961122

Also published as:

 WO9739424 (A1)
 EP0894312 (A1)
 US6014748 (A1)
 US5889941 (A1)
 JP2006072998 (A)

more >>

[Report a data error here](#)

Abstract not available for JP2000508794T

Abstract of corresponding document: **US6014748**

A smart card personalization system maintains a database containing card issuer data format templates, card applications, card operating system commands, and personalization equipment specifications and provides a centralized interface of inputs and outputs to a card issuing process which dynamically adjusts to changes in the issuing process to easily permit a card issuer to change data formats, card applications, card operating systems and/or personalization equipment in a card issuing process. The system interfaces to any card issuer management system, manages the transfer of cardholder data and card applications to the particular personalization equipment used, and maintains statistics for real-time and off-line inquiries to support critical management and reporting functions. Furthermore, the system works with a variety of security methodologies to prevent fraud.

Data supplied from the **esp@cenet** database - Worldwide

(19)日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11)特許出願公表番号
特表2000-508794
(P2000-508794A)

(43)公表日 平成12年7月11日(2000.7.11)

(51)Int.Cl.⁷
G 0 6 K 17/00

識別記号

F I
G 0 6 K 17/00

特マコード* (参考)
B

審査請求 有 予備審査請求 有 (全 65 頁)

(21)出願番号 特願平9-537290
(86) (22)出願日 平成9年4月14日(1997.4.14)
(85)翻訳文提出日 平成10年10月15日(1998.10.15)
(86)国際出願番号 P C T / U S 9 7 / 0 6 2 0 4
(87)国際公開番号 W O 9 7 / 3 9 4 2 4
(87)国際公開日 平成9年10月23日(1997.10.23)
(31)優先権主張番号 6 0 / 0 1 5 , 7 4 3
(32)優先日 平成8年4月15日(1996.4.15)
(33)優先権主張国 米国 (U S)
(31)優先権主張番号 0 8 / 7 5 5 , 4 5 9
(32)優先日 平成8年11月22日(1996.11.22)
(33)優先権主張国 米国 (U S)

(71)出願人 ユービック インコーポレイティド
アメリカ合衆国, ミネソタ 55345, ミネ
アポリス, ベイカー ロード 5909, スウ
イート 580
(72)発明者 トゥシー, デビッド アール.
アメリカ合衆国, ミネソタ 55347, エデ
ン プレーリー, プランチング ホーン
11145
(72)発明者 ホーサー, ウィリアム ダブリュ.
アメリカ合衆国, ミネソタ 55318, チャ
スカ, オータムン ウッズ ドライブ
2750
(74)代理人 弁理士 石田 敬 (外4名)

最終頁に続く

(54)【発明の名称】 スマートカード個人化のシステムおよび装置

(57)【要約】

スマートカード・パーソナル化システムは、カード発行
者側データフォーマット・テンプレートと、カード・ア
プリケーションと、カード・オペレーティングシステム
命令と、パーソナル化用設備の仕様とを保持し、発行プ
ロセスに対する入出力の集中インタフェースを提供して
該発行プロセスの変更をダイナミックに調節すること
により、カード発行プロセスにおけるフォーマット、カー
ド・アプリケーション、カード・オペレーティングシス
テムおよび/またはパーソナル化用設備(130)をカード
発行者が変更することを容易に許容する。任意のカード
発行者側管理システム(150)に対するシステム・インタ
フェースは、使用される特定のパーソナル化用設備に対
するカード保持者データおよびカード・アプリケーショ
ンの転送を管理し、リアルタイムおよびオフラインの照
会に対する統計を維持し、重要な管理および報告機能を
支持する。更に、該システムは種々の安全保障方法によ
り機能し不正を防止する。

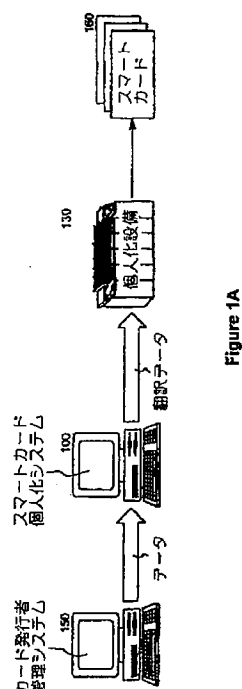


Figure 1A

【特許請求の範囲】

1. パーソナル化用設備の識別子と、カード保持者に対するパーソナル化データと、をカード発行者管理システムから獲得する段階と、

上記パーソナル化用設備の識別子により指定されたデータベース内レコードから、パーソナル化用設備の形式に対する設備特性データを獲得する段階と、

上記形式のパーソナル化用設備に対する設備特性データにより指定されたパーソナル化用設備に対してパーソナル化データを転送しデータ担体を発行する段階と、

を備え、可搬のプログラムされたデータ担体を発行する方法。

2. 前記パーソナル化データを内部フォーマットに変換し、変換されたパーソナル化データは前記パーソナル化用設備に転送される段階を更に備え、請求項1記載の方法。

3. 前記パーソナル化データは、前記カード発行者管理システムにより定義されたフォーマットから、フォーマット・テンプレート・データに従う内部フォーマットに変換される、請求項2記載の方法。

4. 前記カード発行者管理システムにより供給されるデータフォーマットの識別子により指定されたデータベース内の記録から前記フォーマット・テンプレート・データを獲得する段階を更に備え、請求項3記載の方法。

5. 前記カード発行者管理システムから前記フォーマット・テンプレート・データを獲得する段階を更に備え、請求項3記載の方法。

6. 前記カード発行者管理システムにより供給されるアプリケー

ション・プログラムの識別子により指定されたデータベース内アプリケーション・データの記録から前記フォーマット・テンプレート・データを獲得する段階を更に備え、請求項3記載の方法。

7. データ担体の発行に関する情報を収集する段階と、収集された情報から導かれた統計を前記カード発行者管理システムに対し報告する段階とを更に備え、請求項1記載の方法。

8. 前記カード発行者管理システムからアプリケーション・プログラムの識別

子を獲得する段階と、上記アプリケーション・プログラムの識別子により指定されるデータベース内の記録からアプリケーション・データを獲得する段階と、該アプリケーション・データを、前記設備特性データにより指定されるパーソナル化用設備に対して転送する段階とを更に備え、請求項 1 記載の方法。

9. 安全保障の源から安全保障のデータを獲得する段階と、

該セキュリティ・データを、前記設備特性データにより指定されたパーソナル化用設備に対して転送する段階と、

を更に備え、請求項 1 記載の方法。

10. 前記カード発行者管理システムからカード・オペレーティングシステムの識別子を獲得する段階と、

該オペレーティングシステムの識別子により指定されたデータベース内の記録からプログラミング制御命令を獲得する段階と、

該プログラミング制御命令を、前記設備特性データにより指定されるパーソナル化用設備に対し転送する段階と、

を更に備え、請求項 1 記載の方法。

11. 前記カード発行者管理システムからアプリケーション・プログラムの識別子を獲得する段階と、該アプリケーション・プログラム識別子により指定されたデータベース内レコードからアプリケーション・データを獲得する段階と、該アプリケーション・データ

を、前記設備特性データにより指定されたパーソナル化用設備に対して転送する段階とを更に備え、請求項 10 記載の方法。

12. パーソナル化用設備の識別子と、カード保持者に対するパーソナル化データと、をカード発行者管理システムから獲得するカード発行者管理システム・インタフェイスと、

上記パーソナル化用設備の識別子により指定されたデータベース内レコードから、パーソナル化用設備の形式に対する設備特性データを獲得するパーソナル化用設備インタフェイスと、を備え、

該パーソナル化用設備インタフェイスは更に、パーソナル化用設備の形式に対

する設備特性データにより指定されるパーソナル化用設備へパーソナル化データを転送してデータ担体を発行する、

可搬のプログラムされたデータ担体を発行するシステム。

13. 前記システムは更に、前記カード発行者管理システムにより供給されたデータフォーマット識別子により指定されたデータベース内の記録からフォーマット・テンプレート・データを獲得し、パーソナル化データを、該フォーマット・テンプレート・データにより定義されたフォーマットから内部フォーマットに変換し、パーソナル化用設備インタフェイスは変換されたパーソナル化データを前記パーソナル化用設備に転送する、請求項12記載のシステム。

14. データ担体の発行に関して当該システムからデータを収集し、収集されたデータを前記カード発行者管理システムに対し報告する追跡／報告エンジンを更に備えて成る、請求項12記載のシステム。

15. 前記カード発行者管理システム・インタフェイスにより獲得されるアプリケーション・プログラムの識別子により指定されたデータベース内記録からアプリケーション・データを獲得するカード・アプリケーション・インタフェイスを更に備え、且つ、

前記パーソナル化用設備インタフェイスは更に、前記設備特性データにより指定されたパーソナル化用設備へ上記アプリケーション・データを転送する、請求項12記載のシステム。

16. 安全保障源から安全保障データを獲得すると共に該安全保障・データを前記パーソナル化用設備インタフェイスに転送する安全保障管理装置を更に備えて成る、請求項12記載のシステム。

17. 前記カード発行者管理システム・インタフェイスにより獲得されたカード・オペレーティングシステムの識別子により指定されたデータベース内記録からプログラミング制御命令を獲得するカード・オペレーティングシステム・インタフェイスを更に備え、且つ、

前記パーソナル化用設備インタフェイスは更に、上記プログラミング制御命令を、前記設備の特性データにより指定されるパーソナル化用設備に転送する、請

求項 1 2 記載のシステム。

1 8. 前記カード発行者管理システム・インタフェイスにより獲得されるアプリケーション・プログラムの識別子により指定されたデータベース内記録からアプリケーション・データを獲得するカード・アプリケーション・インタフェイスを更に備え、且つ、

前記パーソナル化用設備インタフェイスは更に、上記アプリケーション・データを、前記設備特性データにより指定されるパーソナル化用設備に対し転送する、請求項 1 7 記載のシステム。

1 9. 複数のパーソナル化設備の要素を備える可搬のプログラムされたデータ担体を生成するための、記憶装置に記憶されるデータ構造であって、

各パーソナル化用設備の要素は、一意的なパーソナル化用設備の識別子によりアドレス指定されると共にパーソナル化用設備の形式に対する作用パラメータを指定し、パーソナル化データはデータ担

体を発行する為に使用される形式のパーソナル化用設備に対する送信のために適切にフォーマットされる、データ構造。

2 0. 複数のデータフォーマットの要素を更に備え、

各データフォーマット要素は、一意的なデータフォーマットの識別子によりアドレス指定され、カード発行者により使用されパーソナル化データをフォーマットするテンプレートを指定する、請求項 1 9 記載のデータ構造。

2 1. 複数のカード・オペレーティングシステムの要素を更に備え、

各カード・オペレーティングシステム要素は、一意的なカード・オペレーティングシステムの識別子によりアドレス指定され、且つ、前記パーソナル化用設備への送信のためにプログラミング制御コマンドを指定する、請求項 1 9 記載のデータ構造。

2 2. 複数のアプリケーション・プログラムの要素を更に備え、

各アプリケーション・プログラム要素は、一意的なアプリケーション・プログラム識別子によりアドレス指定され、前記パーソナル化用設備への送信のために特定の形式のアプリケーション・プログラムにより使用されるアプリケーション

・データを指定する、請求項 19 記載のデータ構造。

23. 複数のカード・オペレーティングシステムの要素を更に備え、

各カード・オペレーティングシステム要素は一意的なカード・オペレーティングシステムの識別子によりアドレス指定され、前記パーソナル化用設備への送信のためにプログラミング制御命令を指定する、請求項 22 記載のデータ構造。

24. データストリームを受信すると共にそれに応じて可搬のプログラムされたデータ担体をパーソナル化するパーソナル化用設備

と、

カード発行者管理システムから獲得されるパーソナル化データと、

データフォーマット・テンプレート要素、カード・アプリケーション・データ要素、カード・オペレーティングシステム要素、およびパーソナル化用設備エレメントからなる群から選択される 1 つまたはそれより多いデータ要素を含むデータベースを有するスマートカード・パーソナル化システムと、を備え、

上記スマートカード・パーソナル化システムは、選択されるデータ要素の少なくとも 1 つにより導かれるパーソナル化データを処理した結果としてデータストリームを出力する、

可搬のプログラムされたデータ担体を発行するシステム。

25. カード保持者用パーソナル化データおよび設備特性データを獲得する段階と、

上記設備特性データにより指定されたパーソナル化用設備に対して上記パーソナル化データを転送してデータ担体を発行する段階とを備え、可搬のプログラムされたデータ担体を発行する方法。

26. カード保持者用パーソナル化データおよび設備特性データを獲得し、更に、上記設備特性データにより指定されたパーソナル化用設備に対し上記パーソナル化データを転送してデータ担体を発行するシステム・インタフェース、を備え、可搬のプログラムされたデータ担体を発行するシステム。

27. カード保持者用パーソナル化データおよびパーソナル化手段用特性データを獲得し、更に、上記特性データにより指定されるパーソナル化手段に対し上

記パーソナル化データを転送してデータ担体を発行する手段、を備え、可搬のプログラムされたデータ担体を発行するシステム。

28. パーソナル化手段識別子と、カード保持者に対するパーソナル化データと、をカード発行者管理システムから獲得するシステム・インタフェイス手段と、

上記パーソナル化手段識別子により指定されるデータベース内記録から所定形式のパーソナル化手段に対する特性データを獲得するパーソナル化インタフェイス手段と、を備え、

上記パーソナル化インタフェイス手段は更に、上記形式のパーソナル化手段に対する上記特性データにより指定されるパーソナル化手段に対し上記パーソナル化データを転送してデータ担体を発行する、

可搬のプログラムされたデータ担体を発行するシステム。

29. 前記システム・インタフェイス手段により獲得されるアプリケーション識別子により指定されるデータベース内の記録からアプリケーション・データを獲得するアプリケーション・インタフェイス手段を更に備え、

前記パーソナル化インタフェイス手段は更に、前記特性データにより指定される前記パーソナル化手段に対し上記アプリケーション・データを転送する、請求項28記載のシステム。

30. 前記システム・インタフェイス手段により獲得されるカード・オペレーティングシステム識別子により指定されるデータベース内の記録からプログラミング制御命令を獲得するオペレーティングシステム・インタフェイス手段を更に備え、

前記パーソナル化インタフェイス手段は更に、前記特性データにより指定される前記パーソナル化手段に対し上記プログラミング制御命令を転送する、請求項28記載のシステム。

31. 前記システムは更に、前記カード発行者管理システムにより供給されたデータフォーマットの識別子により指定されるデータ

ベース内の記録からフォーマット・テンプレート・データを獲得し、パーソナリ
化データを、該フォーマット・テンプレート・データにより定義されたフォー
マットから内部フォーマットに変換し、パーソナリ化インタフェイスは変換された
パーソナリ化データを前記パーソナリ化手段に転送する、請求項 28 記載のシス
テム。

【発明の詳細な説明】

スマートカード個人化のシステムおよび装置

発明の分野

本発明はデータ記憶装置に関し、特に、クレジットカード、デビットカード、身分証明カード、および他の取引カードなどの可搬のプログラムされたデータ担体を作成する方法に関する。

発明の背景

ユーザ、顧客または従業員に対して取引カードを発行する組織の数は増加しており、特定の機能または用途に対する要件を満足すべく適合作成されたカードが必要となっている。これらの組織はまた、カード保持者に関するデータをカードに含ませようとしている。既存の取引カードはこのようなデータをカードの背後の磁気ストライプにコード化するが、磁気ストライプにより保持されるデータ量は限られている。新たな形式の取引カードでは、カードのプラスチック部分にマイクロプロセッサ・コンピュータチップを埋設し、カードのデータ記憶容量を相当に増大している。これに加え、チップの種類によってはカード発行者に特有の洗練されたカード応用（アプリケーション）を実行し得ると共に、チップもまた所定型式のオペレーティングシステムを含むことができる。産業界では、チップが埋設された取引カードは可搬のプログラムされたデータ担体と称され、更に一般的には“スマートカード(smart card)”と称されている。スマートカードのチップは、カードの表面が浮彫り加工および／または印刷されると同時に、初期化および／または個人化データによりプログラムされる。

初期化データは3つの主要な種類の情報を備えている：応用（アプリケーション）データ安全保障（セキュリティ）データ、および、印刷されたデータである。アプリケーションデータは、所定のカード用途に対する全てのカードに対して共通であり、アプリケーション・プログラムコードおよび変数を含んでいる。また、安全保障のデータは、カードの不正使用を防止すると共に、通常は“安全保障キー(secure keys)”の形態で提供される。そして、ロゴ、バーコードなどの印刷データ、および、様々の種類の数値情報はカードの表面上に配置される。同

一のデータの幾つかまたはすべてもまた、表面上に浮彫り加工されることができる。更に、カードの表面の一部もしくは全てを、適切な光学読取器によりデータアクセスし得る記憶媒体にするよう光学技術も採用されることができる。

スマートカードはまた、“個人化（パーソナリゼーション）”と称されるプロセスにより個々のカード保持者にとり特定の情報によりプログラムされる。スマートカードに対するパーソナリゼーション情報は、現在における非スマートカードに含まれるパーソナリゼーション情報と同様であるが、それは、カード保持者の氏名、口座番号、カード満了日、および写真などである。その大なる記憶容量により、スマートカードのチップは標準的な取引カードに含まれる基本情報を超過する付加的なデータを含み得るが、これには、個人の署名の図形表示、カード保持者が資格をもつサービスの形式を規定するデータ、及び、これらのサービスについての料金の限度が含まれる。

スマートカードの発行プロセスは、パーソナリゼーションされたカードおよびパーソナリゼーションプロセスの結果を夫々制御すると共にそのレポートを行わねばならない。従って、カード追跡要件を支持する為には多大なレポートファイルおよび監査ファイルを保持せねばならない。

現在、スマートカード発行システムは注文作成されねばならないが、これは、特定のカード・オペレーティングシステムの制御下で特定の形式のスマートカード上にプログラムされる特定のカード・アプリケーションの要件を満足すると共に、カードを発行すべく選択された特定のタイプのパーソナリゼーション設備と互換性を有すべくカードのデータをフォーマットする為である。而して、これらの変数（発行者のアプリケーション、スマートカード／カード・オペレーティングシステム、および／または、パーソナリゼーション設備）のいずれかひとつが変更されたときは、常に発行システム全体を再構成せねばならず、パーソナリゼーションスマートカードを顧客に対して配布する上でカード発行者は多大な時間および費用を負担している。これに加え、現在の発行システムの多くは、プロセスにおける特定のカードのバッチの状況につきカード発行者に対しダイナミックなフィードバックを提供する上で有効な手段を欠いている。

更に、今日使用されているスマートカード発行システムは、カード製造業者もしくはパーソナル化用設備の製造業者のいずれかにより開発される専用の方法を利用する。各製造業者は夫々のカードまたは設備の販売を促進するよう、特定のカード・アプリケーションに対して独自のパーソナル化の解決策を開発すると共に、各解決策は特定のカード発行者に対して固有のものとなっている。これらの独自の解決策は、カードまたは設備の性能を最適化することを意図するものの、更に包含的であると共に任意のカード・オペレーティングシステム、および/または、任意のパーソナル化用設備により行われる作業を受入れる汎用パーソナル化プロセスを許容するものではない。

スマートカードに対する需要が増大するにつれ、複数の形式のスマートカードおよびそれに付随するオペレーティングシステムを取

扱い、種々の形式のスマートカードの任意のものに必要とされるカード保持者データと共に発行者の特定のカード・アプリケーションを書込むよう、任意の形式のパーソナル化用設備の使用をカード発行者に許容するスマートカード発行システムが要求されている。

発明のサマリー

本発明のスマートカード・パーソナル化システムは、カード・アプリケーション・データ、発行者側フォーマット・テンプレート・データ、カード・オペレーティングシステム・データ、および、パーソナル化用設備データを含むデータベースを保持し、発行プロセスに対するカード発行者のインタフェースの変更を要せずに、カード発行者がカード発行プロセスにおいて、カード・アプリケーション、カードおよびカード・オペレーティングシステム、および/または、パーソナル化用設備をダイナミックに変更するのを許容する。

上記スマートカード・パーソナル化システムは可搬のプログラムされたデータ担体すなわちスマートカードを発行するが、これは先ず、カード発行者側管理システムから、データフォーマット識別子 (ID)、カード・オペレーティングシステム識別子、パーソナル化用設備識別子、単一もしくは複数のアプリケーション・プログラム識別子、および、カード保持者用パーソナル化データを獲得するこ

とで行われる。各識別子によりシステムはデータベースなどのデータ構造内に記憶されたデータのアドレス指定が許容される。各カード発行者はそのパーソナリ化データを別個にフォーマットすると共に複数のデータフォーマットを有し得ることから、当該スマートカード・パーソナリ化システムは、複数のカード発行者管理システムとのインタフェースを可能とするデータフォーマット・テンプレ

ートのデータベースを有する。当該システムは、データフォーマット識別子により指定されたデータベース内レコードから、特定のカード発行者により使用されたパーソナリ化データ定義用フォーマット・テンプレートを獲得する。当該システムは上記データフォーマット・テンプレートを使用时、パーソナリ化データをカード発行者のフォーマットから、当該システムの構成要素により認識される内部フォーマットに翻訳する。当該システムはカード・オペレーティングシステム識別子およびアプリケーション・プログラム識別子を使用し、カードに埋込まれたマイクロプロセッサチップ内に予じめ搭載されるオペレーティングシステムに対するプログラミング制御命令、および、アプリケーション・データ、を、ひとつのもしくは複数のアプリケーション・プログラム・形式に対するコードおよび／または変数の形態で上記データベースから獲得する。当該システムはまた、スマートカードを発行するために使用されるべきパーソナリ化用設備に対する設備特性データを、上記パーソナリ化用設備の識別子を用いて獲得する。スマートカードの発行に必要なデータのすべてを当該システムが一旦獲得したなら、該システムは、プログラミング制御コマンド、アプリケーションコードおよび変数、並びに、変換されたパーソナリ化データを、設備特性データにより指定されたパーソナリ化用設備に転送する。

代替的には、カード発行者により何らのデータフォーマット識別子も引渡されない、その理由は、データフォーマット・テンプレートはアプリケーション・データレコード内のデータから導かれ、または、パーソナリ化のフォーマットが当該システムにより使用される内部フォーマットと1対1に対応するからである。カード発行者はまた、データフォーマット・テンプレート・レコードでデータフォーマット識別子を置換え、当該システムがそのフォーマット・レ

コードを参照する必要がなくなるようにすることが可能である。

上記スマートカード・パーソナル化システムの他の一つの特徴は、そのカード管理機能である。該スマートカード・パーソナル化システムはカード発行プロセスに関する情報を収集し、この情報をカード発行者管理システムに対してレポートする。

一方、スマートカードは、チップ内にプログラムされてカードの不正使用を防止するひとつ以上の“安全保障キー”を含み得る。適切な安全保障キー・データはスマートカード・パーソナル化システムにより、カード発行者により保持された安全保障キー・レコードもしくは別のセキュリティ・ソースから獲得され、次に、パーソナル化用設備へ転送される。安全保障源はまた、スマートカード・パーソナル化システムにより使用される安全保障機能も提供し、これにより、当該システムとの間のデータの送信の間において、且つ、スマートカードのパーソナル化プロセスの間にシステム内において、データの完全性および機密性を確かなものにする。

上記スマートカード管理システムは単一もしくは複数のコンピュータ上で実行される一連のソフトウェアモジュールを介して上述の機能を実現する。ひとつのモジュールはカード発行者側管理システム・インタフェイスであるが、該インタフェイスは、データフォーマット識別子、カード・オペレーティングシステム識別子、パーソナル化用設備の識別子、アプリケーション・プログラム識別子、および、カード保持者用パーソナル化データを、カード発行者管理システムから獲得する。カード発行者管理システム・インタフェイスは次に、データフォーマット識別子を用いてフォーマット・テンプレートを獲得するが、これは、パーソナル化データを定義すると共にパーソナル化データを共通の内部データフォーマットに変換するものである。カード・オペレーティングシステム・インタフェイス

・モジュールは、カード・オペレーティングシステム識別子により指定されたカード・オペレーティングシステム形式に対するプログラミング制御コマンドを獲得する。カード・アプリケーション・インタフェイス・モジュールは、アプリケーション・プログラム識別子を用いることによりどの形式のアプリケーション・

プログラムがカード上に配置されるべきかを決定すると共に、指定されたアプリケーションコードおよび変数を獲得する。パーソナル化用機器インタフェース・モジュールが行うべきことは、パーソナル化用設備の識別子により指定されたパーソナル化用機器形式に対する機器特性データの獲得と、更に、機器特性データにより規定された要件に従い、プログラミング制御命令、アプリケーションコードおよび変数、並びに、変換されたパーソナル化データをパーソナル化用設備に転送することである。

報告および安全保障機能は、追跡／報告モジュールおよび安全保障キー管理モジュールにより提供される。

上記スマートカード・パーソナル化システムはコンピュータ記憶媒体内に存在するデータベースなどの基礎データ構造を用い、スマートカードを発行するに必要なデータを構成する。このデータ構造は幾つかの異なる形式のデータ・エレメントから成ると共に、指定されたデータに迅速にアクセスするために“インデックス”または“識別子”を使用する。上記システム内には4つの主要データの要素があり、それは：データフォーマットの要素カード・オペレーティングシステムの要素、アプリケーション・プログラムの要素、および、パーソナル化用設備の要素である。

上記データフォーマット要素は、カード発行者が使用したパーソナル化データのフォーマットを定義するテンプレートを含んでいる。データフォーマット要素は種々のカード発行者に対するデータフ

ォーマット要素を含むデータベース内に記憶されることが可能であり、データフォーマット要素内に記憶された情報はデータフォーマット識別子によりアクセスされる。代替的に、カードが発行されるときにデータフォーマット要素がアプリケーション・プログラム要素内のデータから導かれ、カード発行者により引渡されるアプリケーション・プログラム識別子がデータフォーマットを指定するようにすることが可能である。スマートカード・パーソナル化システムにより使用される内部フォーマットに対しパーソナル化データのデータフォーマットが正確に対応するときは、データフォーマット・テンプレートは論理的に包含され、この

ことは発行のプロセスについて仮想的なデータフォーマットの要素を創出する。

カード・オペレーティングシステム要素は、スマートカード・チップに対するカード・オペレーティングシステムの制御を導くプログラミング制御命令を保持し、カード・オペレーティングシステム識別子によりアクセスされる。

アプリケーション・プログラム要素は、種々のカード発行者に関連するアプリケーションにより必要とされるプログラムコードおよび変数などのアプリケーション・データを含み；アプリケーション・データはアプリケーション・プログラム識別子によりアクセスされる。

種々の形式のパーソナル化用設備に対する作用パラメータは、パーソナル化用設備の要素に記憶され、発行作業の間に使用されるべきパーソナル化用設備の形式に対応するパーソナル化用設備の識別子によりアクセスされる。

上記スマートカード・パーソナル化システムの特異な形態は、カード発行者を支持するが、上述のシステムの全面的な弾力性を必要とするものではない。

上記スマートカード・パーソナル化システムは先行技術の弱点に対処するものであるが、これは、スマートカード・パーソナル化処理に対する入出力の集中インタフェイスであって発行プロセスにおける変更に対応するよう適合するように設計された集中インタフェイスを提供することで行われる。該システムは、任意の発行者管理システムとインタフェイスし、使用される特定のパーソナル化用設備に対するカード保持者データおよびカード・アプリケーションの転送を管理し、リアルタイムおよびオフラインの照会に対する統計を収集して重要な管理および報告機能を支持する。上記システムは発行者データフォーマット、カード・オペレーティングシステム、カード・アプリケーション・プログラム、および、パーソナル化用設備の形式、のデータベースを保持する。このデータベースはシステムに対し任意のデータの組合せまたは順列を可能にし、従って、発行者に対し出荷を行う上での経費および時間を改善することができる。更に、上記システムは種々のカード安全保障の方法とインタフェイスし、不正使用を減少させる。

図面の簡単な説明

図1Aは、スマートカード・パーソナル化システムを組み入れたスマートカー

ド発行プロセスを示すブロック図である。

図 1 B は、図 1 A に示されたスマートカード・パーソナル化システムに対する入出力接続の機能的ブロック図である。

図 1 C は、図 1 B に示されたスマートカード・パーソナル化システムの一実施例を備えるソフトウェアモジュールおよびデータ構造の機能的ブロック図である。

図 2 は、スマートカードに使用されるキーを管理する安全保障・モジュールを付加した、図 1 C の実施例の機能的ブロック図である。

図 3 は、複数の形式のカードおよびパーソナル化用機器を管理する最小限の配置構成を示すスマートカード・パーソナル化システムの別実施例の機能的ブロック図である。

図 4 は、複数のカード・オペレーティングシステムを管理するモジュールを付加した、図 3 の実施例の機能的ブロック図である。

図 5 は、安全保障・モジュールを付加した図 4 の実施例の機能的ブロック図である。

図 6 は、複数のカード・アプリケーションを管理するモジュールを付加した図 3 の実施例の機能的ブロック図である。

図 7 は、安全保障・モジュールを付加した図 6 の実施例の機能的ブロック図である。

図 8 は、上記スマートカード・パーソナル化システムの機能を実現するコンピュータ・ソフトウェアの上位レベルのフローチャートの図である。

図 9 は、ソフトウェアモジュールおよびデータレコードを使用するスマートカード・パーソナル化システムの代替実施例の機能的ブロック図である。

図 10 は、図 9 に示されるスマートカード・パーソナル化システムの実施例の機能を実現するコンピュータ・ソフトウェアの上位レベルフローチャートの図である。

図 11 は、図 9 に示されるスマートカード・パーソナル化システムの実施例に

より使用されるカード構造テンプレート・レコードのデータフィールドの図である。

図 1 2 は、図 9 に示されるスマートカード・パーソナル化システムの実施例により使用されるデータフォーマット・テンプレート・レコードのデータフィールドの図である。

図 1 3 は、図 9 に示されるスマートカード・パーソナル化システムの実施例により使用されるカード・アプリケーション・データ・レコードのデータフィールドの図である。

図 1 4 は、上記スマートカード・パーソナル化システムにより追跡される項目の例を示すレポートフォーマットの図である。

実施例の記述

以下の実施例の詳細な説明においては添付図面を参照するが、これらの図面は本明細書の一部を成すと共に本発明が実施される特定の実施例を例示している。これらの実施例は当業者が本発明を実施し得る如く十分に詳細に記述されているが、本発明の精神および範囲から逸脱することなく他の実施例を活用すると共に構造的、論理的および電気的な変更を行い得ることは理解されよう。従って、以下の詳細な説明は限定的なものと解釈してはならず、本発明の範囲は添付の請求の範囲によってのみ定義される。

図面中における参照番号の先行数字は通常は図面番号に対応するが、複数の図面に現われる同一構成要素は同一の参照番号で識別される。

スマートカードの発行

通常のクレジットカードなどの標準的な取引カードは殆どの人々に馴染んでいる。取引カードは通常、カードの表面上に印刷および／または浮彫り加工された氏名および口座番号などのカード保持者に関する情報を有している。また、取引カードは、カード保持者のデータがコード化された磁気ストライプを含むことも多い。各取引カードに対してカード保持者データを印刷／エンボス加工／コード化するプロセスは“個人化（パーソナル化）”として知られている。また、各取引カードには“初期化”として知られた

処理が行われるが、該処理においては、バッチにおけるすべてのカードに対して共通な発行者識別子およびバッチ番号等の情報がカード上に配置される。

スマートカードは、カードのプラスチック内にコンピュータ・マイクロプロセッサ・チップが埋め込まれてカードのデータ記憶容量を相当に増大させるという点で標準的な取引カードと相違している。また、スマートカードの種類によっては、カードの製造業者が幾つかの可能なカード・オペレーティングシステムの一つをチップに予じめ搭載し、該オペレーティングシステムがパーソナル化プロセスの期間にチップのプログラミングを制御している。これに加え、チップの種類によっては、カード発行者に特定の非常に複雑なカード・アプリケーションが実行されることが可能である。

スマートカードに対する初期化データは3つの主要な種類の情報を備えている：アプリケーションデータ、安全保障データ、および、印刷されたデータである。アプリケーションデータは、所定のカード用途に対する全てのカードに対して共通であると共に、チップ内にプログラムされるアプリケーション・プログラムコードおよび変数を含む。また、セキュリティ・データは、通常は安全保障キーもしくは安全保障機能を提供し、カード上のデータを有効化し、且つ、カードの不正使用を防止するものである。而して、ロゴ、バーコードなどの印刷データ、および、様々の種類の数値情報はカードの表面上に配置される。同一のデータの一部もしくは全ても、表面上に浮彫り加工され得る。更に、スマートカードの表面の一部を、適切な光学読取器によりデータアクセスし得る記憶媒体とすべく、光学技術も採用され得る。

スマートカードに対するパーソナル化情報は、非スマートカードに現在含まれるカード保持者氏名、口座番号、カード満了日、およ

び写真などのパーソナル化情報と類似している。その記憶容量が大きいことから、スマートカードのチップは標準的な取引カードの基本情報を越える付加的データを含み得るが、これには、個人の署名の図形表示、カード保持者に付与されたサービスの種類を定義するデータ、及び、これらのサービスに対する口座限度が含まれる。

スマートカードパーソナル化のシステム

図1 Aは、本発明のスマートカード・パーソナル化システムの実施例を取入れたスマートカード発行プロセスの構成要素を示している。スマートカード・パーソナル化システム100は、（通常はカード発行者専有の）カード発行者側管理システム150からデータを受理し、データをデータストリームに翻訳し、スマートカード160をパーソナル化するパーソナル化用設備130にデータストリームを出力する。カード発行者管理システム150は、カード保持者データを管理し、発行すべきカードの形式と、カード内に書込まれるべきカード・アプリケーションと、特定のカード保持者に対しカードを発行する上で使用すべきパーソナル化用設備とを決定する。カード発行者管理システムは図1 Aに示されるようにコンピュータプログラムであることが多いが、スマートカード・パーソナル化システム100は、電話のキーパッドからの人間による入力などの代替的入力を受理することもできる。

スマートカード・パーソナル化システム100は、コンピュータ内で実行されるソフトウェアプログラムとして図1 Aに示される。以下に記述されるように、スマートカード・パーソナル化システム100は、種々の形式のカードおよびカード・オペレーティングシステム、カード・アプリケーション、並びに、パーソナル化用設備を定義するデータベースレコードにアクセスする。

ソフトウェアおよびデータベースの論理機能は、クライアント／

サーバネットワークにおけるコンピュータに分散させてもよく、または、単一プロセッサに集中化しても良い。これらの機能はまた、各プロセッサを離間結合するよう使用される標準的ローカルエリアネットワーク、ワイドエリアネットワーク、専用電話線または他の通信手段を介して接続されるプロセッサ間に分散され得る。上記ソフトウェアプログラムは、UNIX、Windows 95(登録商標)もしくはWindows NT(登録商標)、および、工業標準ワークステーションおよび／またはパーソナルコンピュータ・ハードウェアなどのオペレーティングシステム上で実行される。

システム100は、パーソナル化用システム130として図1 Aに集散的に示された

、カードプリンタ、浮彫り加工装置、および、集積または付加されたスマートカードインタフェース装置を制御する。パーソナル化用機器130はまた、大容量カードプリンタ／エンボス加工器、小容量カードプリンタ／浮彫り加工器、現金自動預け払い機(ATM)、POS端末、無人キオスク、パーソナルコンピュータ、ネットワークコンピュータ、およびオンライン通信装置などの装置を表している。多くのカード発行者は既存の非スマートカードパーソナル化用設備に投資を行っていることから、新たなスマートカードパーソナル化用設備の全体を購入するのではなく、代わりに、自身の既存のパーソナル化用設備にスマートカードインタフェース装置を追加するが、該インタフェース装置がカードのチップをプログラムする一方でそれまでの装置は印刷および浮彫り加工機能を達成するものである。斯かる配置構成においては、スマートカード・パーソナル化システム100を実行するコンピュータシステムすなわち“ホスト”は、これらの装置の両方もしくは一方のみに物理的に接続され得る。後者の場合、ホストは直接接続された方の装置を制御すると共に、他方に対する論理接続を有する。但し、各装置とホスト

との間の物理的接続は、装置の製造業者および型式により変更される。一般的な業界標準接続としては、RS232C、SCSI（小型コンピュータシステム・インタフェース）、イーサネット、および、シリアルTTL（トランジスタートランジスタ論理）が挙げられる。これに加え、装置に依っては専用のバス接続が必要となる。

スマートカード・パーソナル化システム100、カード管理システム150および装置130の間の接続は、標準的ローカルエリアネットワーク、ワイドエリアネットワーク、専用電話線、または、データの転送に使用される他の遠隔通信インフラストラクチャ、を介して実現され得る。スマートカードをパーソナル化するときのこのような遠隔接続の使用は、Laingほか1996年7月9日に発行された米国特許第5,524,857号に記述されている。代替的な接続は当業者にとり明らかであり、本発明の範囲内である。

図1Bはスマートカード・パーソナル化システムの一実施例のブロック図であり、スマートカード・パーソナル化システム100とスマートカードを発行するカード発行組織により採用される機能との間の論理接続を示す。カード発行組織に

より保持されるカード保持者データは、氏名、口座番号、カード満了日および適用サービスなどの、個々のカード保持者に関する情報を含む。カード発行者管理システム150に対してカード保持者データを入力する種々の方法は、図1Bにおいてカード保持者データ152として破線で示される。カード発行者管理システム150は、磁気テープ、フロッピーディスク、もしくはCD-ROMなどのコンピュータ媒体によりカード保持者データを受理することができる。代替的に、カード保持者データ152はオンライン接続を介して入力され得るが、それは、汎用の交換式電話網、パケット式交換網すなわちインターネット、専用線、または、ケーブル/衛星テレビ信号などである。当業者であれば、シス

テム150に対してカード保持者データ152を入力する付加的な手法は明らかであろう。

カード発行者管理システム150に加え、カード発行者は典型的に既存の報告機能154を有し、該機能により、スマートカード・パーソナル化システム100は該システム100により保持された統計的情報をカード発行者が吟味することができようインタフェイスを行う。同様にカード発行者により提供されると共に安全保障キー管理装置111および安全保障キー・データベース128として示される外部安全保障源は、カード発行者管理システム150およびスマートカード・パーソナル化システム100と協働して作用する安全保障機能を提供する。図1Bはまた、付加されたスマートカードインタフェイス装置を有するカード発行者を支持するスマートカード・パーソナル化システム100の代替的实施例をも示す。システム100は、パーソナル化情報の一部をそれまでのパーソナル化用機器130に導き、残りのデータを、チップをプログラムするスマートカードインタフェイス装置132内のポストプロセッサ132に導く。これらの機能は以下に詳述する。

以下の図面に示されるスマートカード・パーソナル化システム100に対するソフトウェアプログラムの実施例は、発行プロセスの特定部分を各々実行するモジュールによるコードモジュールの組合せとして機能する。これらの実施例において、各モジュールは定義された入力および出力プログラム呼出により連結されると共に、データ構造内に記憶されたデータに対するアクセスを提供する標準的な

データ照会命令によりデータ構造に連結される。但し、各モジュール間、および、各モジュールとデータ構造との間の通信プロトコルは、各モジュールが記述された言語、および、データベースを支持するよう採用される基本的なデータ管理システム、に依存して変化

する。

図1 Cは、外部安全保障機能を備えない、図1 Bのスマートカード・パーソナル化システム100の更に詳細なブロック図である。図1 Cはソフトウェアモジュールとデータベースレコードとの間の内部接続を示し、これにより、スマートカードを発行する場合においてスマートカード・パーソナル化システム100は、複数の形式の発行者側データフォーマット、カード・オペレーティングシステム、カード・アプリケーションおよびパーソナル化用設備を組合せ得ることになる。

スマートカード・パーソナル化システム100は、カード発行者管理システム150に対し、顧客向きにされたカード発行者管理インタフェイス101を提供する。この実施例においては、カード発行者管理システム150はパーソナル化データをカード保持者データベース152からシステム100に対して引渡す。システム100内の各ソフトウェアモジュールは、特定の内部フォーマットでパーソナル化データが引渡されることを期待する。パーソナル化データは、上記ソフトウェアモジュールにより期待された内部フォーマットとは異なることが多いカード発行者定義の外部フォーマットであることから、パーソナル化データはシステム100によりデータフォーマット・テンプレートをを用いて内部フォーマットに変換される。システム100はカード発行者により引渡されたデータフォーマット識別子を介してデータフォーマット・テンプレートを獲得しても良く、システム100はこれを使用して、選択的データフォーマット・テンプレート記録120とカード発行者管理システムインタフェイス101との間の選択的接続として示された記録120（図1 Cに破線で示されるもの）を獲得する。代替的に、カード発行者は、データフォーマット識別子の代わりにデータフォーマット・テンプレート・レコードをシ

ステム100に引渡す。別の実施例においては、データフォーマット・テンプレ

トは、カード・アプリケーション・データベース124とカード発行者管理システムインタフェイス101との間の選択的接続として示され、発行者により引渡されたアプリケーション・プログラム識別子であるカード・アプリケーション記録124から導かれ得る。

図1Cの更なる代替的实施例においては、カード・アプリケーション記録の一部としてセキュリティ機能をスマートカード・パーソナル化システム100に引渡すことにより、セキュリティ機能はシステム100の内部に提供される。

パーソナル化データフォーマットが内部フォーマットと合致するという更なる代替的实施例もまた、図1Cに示されている。この実施例においては外部フォーマットと内部フォーマットとの間の変換は不要であることから、データフォーマット・テンプレートは何ら必要とされず、従って、データフォーマット記録120と、カード発行者管理システムインタフェイス101およびデータフォーマット記録120の間の接続と、カード・アプリケーション・データベース124と、は示されていない。データフォーマット・レコード120は複数のテーブルから成ることができるが、これらは、パーソナル化データの適切な解析、もしくは、カード保持者データ記録のフィールドが現われる順番を示す単純なリストに関してシステム100に指示を与えるものであり、当業者には自明であろう。上述したパーソナル化データのフォーマットを決定する種々の代替の手順は、本明細書中に記述されるスマートカード・パーソナル化システム100の全ての実施例において自明なものである。

カード発行者管理システム150により与えられたカード識別子を用い、カード・オペレーティングシステム・インタフェイス・モジ

ジュール103は、発行されつつある形式のカードに埋設されたマイクロプロセッサチップに対するカード・オペレーティングシステム122に特有のプログラミング制御コマンドを検索する。プログラミング制御命令は、カード発行者により選択されたパーソナル化データおよび単一もしくは複数のカード・アプリケーションによりチップのコード化を行わせる。

各カード・アプリケーションはプログラムコードおよび可変データを備えるが

、可変データは、アプリケーション・データ124としてデータベース内に記憶されると共にアプリケーション・プログラム識別子により指定される。カード発行者管理システム150はひとつ以上のプログラムアプリケーション識別子をシステム100に引渡し、これは、対応するアプリケーション・データ124を獲得すべくカード・アプリケーション・インタフェース・モジュール105により使用される。

カードのバッチを発行すべくカード発行者が使用を企図するパーソナル化用設備は、パーソナル化用設備の識別子により定義される。パーソナル化用設備インタフェース・モジュール107は、パーソナル化用設備の識別子に対応するパーソナル化用設備130の形式に特有の設備特性データ126を獲得する。パーソナル化用設備インタフェース107はまた、プログラミング制御コマンド、アプリケーションコードおよび変数、並びに変換されたパーソナル化データをも獲得し、設備特性データ126により指定されたパーソナル化用設備130に対してこれらのデータの全てを転送し、スマートカードを発行する。

システム100の代替的实施例は、スマートカード・プログラミング装置により既存のパーソナル化用設備を拡張したカード発行者を支持するが、この拡張は、パーソナル化用設備インタフェース107

により、変換されたパーソナル化情報の部分集合をそれまでのパーソナル化用設備130に導くと共に、データの残存部分をスマートカード・プログラミング装置のポストプロセッサ132に導くことで行われる。

スマートカード・パーソナル化システム100はまた、追跡／報告モジュールすなわちエンジン109をも提供するが、該エンジン109は、システム100内の他のモジュールから統計的情報を収集すると共に、ハードコピー・報告154としての出力、または、カード発行者管理システム150内の報告機能への入力のために統計的情報をフォーマットする。この統計的情報はリアルタイムで収集されつつあることから、カード発行者管理システム150は追跡／報告モジュール109に対してインタラクティブに照会を行い、実行中のスマートカード・パーソナル化システムに関する統計を獲得する。追跡／報告モジュール109により監視される項目の例は、図14に示されている。

図2に示される代替的实施例において、スマートカード・パーソナリ化システム100は、安全保障キー管理装置・モジュール111および安全キー・データベース128の形態の安全保障源を含んでいる。スマートカードが製造される時、その販売者はチップに安全保障構造を含ませ、無権限プログラミングを防止する。安全保障構造の実現は通常、チップにプログラムされるアプリケーションに依存する。例えば、値記憶アプリケーション内にプログラムされた安全保障キーは、健康管理アプリケーションにプログラムされた安全保障キーと異なるものである。また、セキュリティ構造の実現は、カードの形式に依っても変更され；或るカードはチッププログラミングを可能とする単一の安全保障キーを必要とする一方、他のカードはチッププログラミングを可能とすると共に付加的な安全保障機

能を実現する複数の安全保障キーを必要とする。図2は、複数の安全保障キーを要するカードの安全保障構造とインタフェイスを行うときの安全キーマネージャ111の基本機能を示している。

図2に示される如く、安全保障キー・データはスマートカード・パーソナリ化システム100の外部の安全キー・データベース128内に記憶されると共に、カード発行者もしくは他の安全保障源により保持される。更に多くのもしくは更に少ない安全保障キーを処理すると共にスマートカード・パーソナリ化システム100自体により管理される安全保障キー・データベースとインタフェイスすべく安全保障キー管理装置111を拡張することは、特定のカード発行アプリケーションにおいて用いられるアプリケーション、オペレーティングシステム、およびパーソナリ化用設備に依存するものであり、当業者には自明であろう。

安全保障キー管理装置111はまた、安全保障キー・データ認証、データの完全性、およびデータ機密性を確かなものとする付加的なメカニズムも提供する。一実施例において、安全保障キーデータ認証は種々の暗号化方法を実現することで行われる。安全保障キーのデータの完全性は、有効ソースから送信および受信されつつある安全保障キー・データを確かなものとする公開鍵を用いるデジタル署名メカニズムにより達成される。安全保障キー・データの機密性は送信データを秘密鍵で暗号化することにより確かなものとされるが、この秘密鍵はデータ受信

者により共有されると共に受信後にデータを解読すべくデータ受信者により使用されるものである。

システム100が安全保障キー・データベース128から安全保障キー・レコードを受けた後、安全保障キー管理装置111は、カード・オペレーティングシステム・インタフェイス103およびカード・アプリケーション・インタフェイス105と協働し、安全保障キー認証

、データの完全性およびデータ機密性の機能を実現する。システム100は次に、パーソナル化用設備インタフェイス107を介し、安全保障キー・データを他のカードデータと共にパーソナル化用設備130に転送する。

代替の実施例においては、安全保障キーマネージャ111は安全保障情報をスマートカード・パーソナル化システム100の他のモジュールに引渡す。例えば、PIN（個人識別子番号）コードなどのカード保持者データの部分は、スマートカード・パーソナル化システム100に対してデータを引渡す前にカード発行者管理システム150により暗号化され得る。カード発行者管理システムインタフェイス101は安全保障キーマネージャ111を介して安全保障キー・データベース128から暗号化用キーを検索すると共に、PINコードをコード化もしくはプログラミングする前のデータを磁気ストライプおよび／またはチップ内に復号する。

更なる代替の実施例において、安全保障キーの管理装置111は、必要なセキュリティ機能を供給する外部安全保障源に対するゲートウェイ接続を提供する、スマートカード・パーソナル化システム100内へのコード“フック(hook)”である。このような外部安全保障源の例は、第三者により記述されて安全保障キー・データベース128と同様に安全キーおよび／または安全保障機能の安全保障・データベースを管理する安全保障管理プログラムである。安全保障機能は、安全保障管理装置により実行される外部ルーチン、または、そのときにスマートカード・パーソナル化システム100により実行されて所要のセキュリティ機能を提供すべく安全保障管理装置により引渡されたコードモジュール、またはその両者、であり得る。

図3は、スマートカード・パーソナル化システム100の最小限の配置構成を示

している。この実施例においては、カード発行者管理

システムインタフェイス101およびパーソナル化用設備のインタフェイス・モジュール107のみがソフトウェアで有効とされている。この実施例はスマートカード・パーソナル化システム100が非スマートカードをパーソナル化するのを許容していることから、2個の別体のパーソナル化システムを用意するコストを節約する一方、複数のデータフォーマットおよび複数の形式のパーソナル化用設備をカード発行者が使用することを許容する。図3はまた、図1Cに関し上述した追跡／報告モジュール109を含む付加的な代替的实施例も示している。

更なる代替的实施例においては、図3に示されたスマートカード・パーソナル化システム100は、パーソナル化用設備130として光学的コード化設備が使用されるときにデータを光学的取引きカードにコード化する。

図4および図5は、カード発行者がスマートカード・チップ上にカード・アプリケーションをプログラムしないときに実現される更なる代替的实施例を示している。これらの実施例によればカード発行者は、スマートカード・パーソナル化システム100を再構成すること無く、複数の形式のパーソナル化用設備に必然的に多くの種類のオペレーティングシステムと共に複数のカード形式を発行することが許容される。図1Cに関して上述した如く、図4は報告およびポストプロセッシングを支持するモジュールを含んでいる。図5は図4の実施例を示しているが、パーソナル化用設備130に送信を行うカード・オペレーティングシステム・インタフェイス103に対してセキュリティを与える安全保障キー管理装置モジュール111が付加されている。

同様に、図6および図7は、スマートカード上のチップをカード・アプリケーションに対するデータ記憶装置としてのみ使用するこ

とから、チップ上で実行されるオペレーティングシステムを有さないカード発行者を支持する実施例を示している。スマートカード・パーソナル化システム100は、複数の形式のパーソナル化用設備により発行された複数のカード形式に対する複数のカード・アプリケーションを支持する。図6および図7は、安全保障キ

ー管理装置111がカード・オペレーティングシステム・インタフェイス103の代わりにカード・アプリケーション・インタフェイス105に対して安全保障キーおよび／または機能を提供するというを除き、図4および図5に類似している。

図8は、上述のスマートカード・パーソナル化システム100の機能を実現するソフトウェアの一実施例に対する上位レベルのフローチャートである。ソフトウェアはブロック801において、取引カードのバッチに対してカード発行者管理システムから発行されるべきパーソナル化用設備の識別子を獲得する。発行されるべきカードの形式に依存して、ソフトウェアはプログラムアプリケーション識別子および／またはカード・オペレーティングシステム識別子も同時に獲得する。ソフトウェアは次に、上述の処理の一つを介して、パーソナル化データのフォーマットに対応する特定のデータフォーマット・テンプレートを獲得する（ブロック803）。ブロック805において上記システムは、パーソナル化用設備の識別子により指定されるパーソナル化用設備のレコードから、カードのバッチを発行する為に使用されるべきパーソナル化用設備に対する設備の特性を獲得する。

もしカード・オペレーティングシステム識別子がカード発行者管理システムにより引渡されたのであれば（ブロック807）、ソフトウェアはブロック809にてカード・オペレーティングシステム識別子に対応するカード・オペレーティングシステム・データベース記

録からプログラミング制御命令を検索する。ブロック811および813は、カード・アプリケーションに対して同様の論理を実施し、データベースからコードおよび／または変数などのアプリケーション・データを検索する。この点において、当該ソフトウェアはバッチ内のカードの全てに対して必要な共通データを既に獲得しており、且つ、個々のカード保持者に対してカードを発行するロジックを介してのループを開始する。

カード発行者管理システムは単一のカード保持者に対するパーソナル化データをソフトウェアに引渡し（ブロック815）、該ソフトウェアは、データ項目をデータフォーマット・テンプレートにより定義されたフォーマットから、スマートカード・パーソナル化システムのモジュールにより使用される内部フォーマット

に変換する（ブロック817）。もしカードチップが安全保障キーを要する安全保障の構造を含むのであれば（ブロック819）、ソフトウェアは安全保障キー機能を実施するに必要な安全保障キー・データをブロック821にて適切な安全保障キー・ソースから獲得する。

ソフトウェアはいまや、パーソナリ化用設備にデータを転送してカードをプログラムする用意ができています。もしカードが安全保障キーにより保護されているのであれば、安全保障キー機能が実施されると共に安全保障キー・データはブロック823にて転送される。次に、もし該当するのであれば、チップ・オペレーティングシステムに対するプログラミング制御コードが転送され（ブロック825および827）；次に必要であればアプリケーションコードおよび／または変数が転送される（ブロック829および831）。最後に、内部フォーマットに変換されたカード保持者のパーソナリ化データが転送される（ブロック833）。

データがカードに転送された後、ブロック839にてソフトウェア

はカード発行者管理システムに対して自身が収集する統計用の適切な値を付加する。もし同じバッチにおいて発行されるべき更なるカードが残存しているのであれば（ブロック841）、ソフトウェアはブロック815に戻り、次のカード保持者に対するパーソナリ化データを獲得する。さもなければ、ソフトウェアは、別のバッチのカードをカード発行者管理システムが発行するか否かを決定し（ブロック843）、且つ、ブロック801に戻り、新たなバッチに対するサイクルを反復するに必要な情報を獲得する。発行されるべき更なるカードが無ければ、ソフトウェアは処理を終える。

スマートカード・パーソナリ化システム100に対してカード発行者管理システム150が必要なデータを引渡すメカニズム、および、スマートカード・パーソナリ化システムがカード発行者管理システムからのデータを処理する順番は、本発明の範囲を越えること無く変更し得る。システム100が図9および図10に示された代替の実施例のように作用する特定の環境により、異なる配置構成が必要になる。

図9において、安全保障・モジュール911は、図1Bに111および128として示

される安全保障管理装置940および安全保障データベース942などの安全保障・ソースに対するスマートカード・パーソナル化システム100へのゲートウェイとして作用する。安全保障管理装置940は安全保障・データベース942へのアクセスを制御すると共に安全保障・ゲートウェイ911へ接続し、スマートカード・パーソナル化システム100に対して必要な安全保障機能を実現する。安全保障・ゲートウェイ911はカード発行者管理システム・インタフェイス901に連結され、これにより該インタフェイス901は、カード発行者管理システム950により暗号化フォーマットで引渡されたパーソナル化データを解読することを安全保障管理装置940に

対して要求し得るようになる。安全保障・ゲートウェイ911はまたカード・アプリケーション・インタフェイス903およびカード・オペレーティング・インタフェイス905とも連結されることから、それは図2に関して上記で説明した如く必要な安全キーおよび／または安全保障機能を提供し得る。

更に、図9に示されたスマートカード・パーソナル化システム100の実施例は、カード識別子を用いてカード・オペレーティングシステム924に特有のプログラミング制御命令を獲得する前に、アプリケーション・プログラム識別子により指定されたアプリケーション・データ922を獲得する。この実施例では、カード・オペレーティングシステム924および設備特性データ926に対するプログラミング命令を検索する前にパーソナル化データおよびアプリケーション・データが内部フォーマットに変換されるのが許容されることから、各スマートカードの処理が高速化される。

一方、標準的な取引きカードは、該カードの表面に印刷および浮彫り加工されたデータ、および／または、カードの磁気ストライプにコード化されたデータを有している。而して、スマートカードでは、データはマイクロプロセッサ内の内部メモリ領域にも記憶され得る。また、カードの表面上、磁気ストライプ内、および、チップメモリ内に同一のデータが配置され得る。カード内およびカード上のデータの厳密な配置構成は、発行されつつあるスマートカードの形式およびカード発行者の要求に依存して変化する。

図10は図9に示される実施例の高いレベルのフローチャートであり、図11、図12および図13と協働し、スマートカード・パーソナル化システム100を実現すべく異なるメカニズムが如何にして使用され得るかを示している。カード発行者管理システム950はスマートカードの配置構成を定義するカード構造テンプレートをブ

ロック1001にてスマートカード・パーソナル化システム100に引渡す。

図11は、カード構造テンプレート・レコード1100に対するデータ・レイアウトの一実施例を示している。マイクロプロセッサチップ識別子1101および（存在すれば）カード・オペレーティングシステム識別子1102は、発行されるべきスマートカードの形式に特有のものである。マスタファイル定義1103は、チップソースおよびチップが変更された最新日などの制御情報を含んでいる。システムファイル定義1104、1105、1107は、チップのメモリ内のシステムファイルの位置に対するアドレスを含んでいる。これらのシステムファイルはカード・オペレーティングシステムにより使用されると共に、カードおよびアプリケーションに対するPINコードおよびアルゴリズムテーブルを含んでいる。図11に示された実施例においては、マスタファイルおよびシステムファイルは国際標準化機構(ISO)指示番号7816-4に準拠している。

カード構造テンプレート・レコード1100の次の3つのセクションは、カードの表面および磁気ストライプのデータの配置構成を定義する。もしカード保持者の写真1109などの情報がカード上に印刷されるべきであれば、斯かるデータをカードの表面に印刷する箇所はカード発行者管理システム950によりカード構造テンプレート・レコード1100の印刷テンプレートに引渡される。同様に、データをエンボス加工するカード表面の位置がエンボス加工テンプレートに引渡されると共に、磁気ストライプにコード化されるべきデータの配置構成は磁気ストライプ・テンプレートに引渡される。エンボス加工データはカード構造テンプレート・レコード1100内において、カード保持者氏名(EMName)1111、口座番号(EMAct)1113、および満了日(EMXdat)1115として示され、且つ、磁気ストライプデータは口座

番号(MSAcct)1117および満了日(MSXdat)1119により示されている。印刷、エンボス加工および磁気ストライプの各テンプレートにおけるデータ項目の個数はカード発行者により望まれるスマートカードの配置構成に依存して変化するが、当業者であれば自明であろう。

もしカード発行者がスマートカードのチップ内にカード・アプリケーションのプログラムを望むのであれば、カード発行者はアプリケーション・プログラム識別子をカード構造テンプレート・レコード1100のセクション1121、1123、1125内でアプリケーション・プログラム識別子をスマートカード・パーソナリゼーションシステム100に引渡す。各アプリケーションはそれに伴う特定の安全保障機能を有することもあり(1127、1129、1131)、且つ、その情報もまたカード発行者管理システム950により引渡される。カード構造テンプレート・レコード1100はまた、スマートカードを発行すべく使用されるパーソナリゼーション設備に対するパーソナリゼーション設備の識別子1123も含んでいる。

代替の実施例においてはスマートカード・パーソナリゼーションシステム100は共通使用されるカード構造テンプレート・レコードを内部データベースに記憶することから、カード発行者管理システム950は、特定のバッチのカードに対し、使用されるべきカード構造テンプレート・レコードを指定するカード構造テンプレート識別子のみを引渡すことが必要である。

スマートカード・パーソナリゼーションシステム100はブロック1003にて、カード発行者により指定された予定義箇所から、パーソナリゼーションデータに対するデータフォーマット・テンプレートを獲得する。もしカード発行者がシステム100に対して既にデータフォーマット識別子を引渡していれば、データフォーマット識別子に対応するデータフォーマット・テンプレート・レコードはデータフォーマット・デ

ータベース920から検索される。代替的に、カード発行者はデータフォーマット・テンプレート・レコード自体を引渡しても良い。システム100に対してデータフォーマット識別子もデータフォーマット・テンプレート・レコードも引渡されないときには、パーソナリゼーションデータのフォーマットは以下に更に詳述する如くカード・アプリケーション・データにより決定される。

データフォーマット・テンプレート・レコードの一例が図12に示されている。データフォーマット・テンプレート・レコード1200はカード保持者データベース952内のパーソナル化データレコードの仮想的レイアウトを定義しており、口座番号1201が第1フィールドであり、カード保持者氏名1202は第2フィールドであり、カードの満了日1205が第3フィールドである。一実施例において、パーソナル化データレコードはコンマ区切りレコードであることから、レコードフォーマットを定義する上で必要とされるデータフィールド長は存在しない。従って、図12に示されたデータフォーマット・テンプレート・レコード1200は、スマートカード・パーソナル化システム100に対するコンマ区切りパーソナル化データレコードの以下の例の構造を完全に定義している：133444999922, Mary Jane Smith, 0299。

スマートカード・パーソナル化システム100はブロック1007にて、もしあれば、カード発行者管理システム950により引渡されたアプリケーション・プログラム識別子に対応して、単一もしくは複数のカード・アプリケーションに対するアプリケーション・データ922を獲得する。もしアプリケーション・プログラム識別子が引渡されなければ、スマートカード・パーソナル化システム100は既定アプリケーション・データを獲得する（ブロック1008）。アプリケーション・プログラム識別子に対応するカード・アプリケーション・

データ・レコード内の既定値および／またはアプリケーション・データは、カード構造テンプレート・レコード1100の対応セクション、即ち、1121、1123、1125に挿入される。

図13には、カード・アプリケーション・データ・レコードのレイアウトの一実施例が示されている。カード・アプリケーション・データ・レコード1300の第1フィールドは、アプリケーション名1301である。コンピュータに基づく他のアプリケーション・プログラムと同様に、カード・アプリケーションは、現金自動預け払い機などの外部ソース、または、マイクロプロセッサのメモリ内にコード化されたデータファイルなどの内部ソースからのデータを処理する。スマートカードを使用すると、マイクロプロセッサにより適切なアプリケーションが実行さ

れる一方、該アプリケーションはデータを検索もしくは蓄積すべく内部ファイルにアクセスする。内部データにアクセスすべく、カード・アプリケーション・データ・レコードは、チップメモリ内のアプリケーションファイルへのポインタ(1302, 1305, 1307)と、アプリケーションファイル内のフィールドの位置を含んでいる。フィールドの幾つかは、カードが発行されるときにカード保持者データベース952からのデータにより初期化される。アプリケーション・データ1300は、チップメモリ内に配置されたカード保持者ファイルに対するアドレス1303を含むと共に、3つのフィールドを含むものとしてカード保持者ファイルを定義する：カード保持者氏名(ICName)1309、口座番号(ICAcct)1311および満了日(ICXdat)1313である。付加的な内部データは他のアプリケーションファイル内に記憶されると共に、これらの付加的ファイルのレイアウトもまたアプリケーション・データ1300により定義される。

もしスマートカード内に埋設されたチップがカード構造テンプレート・レコードにより指定されたオペレーティングシステムを含む

のであれば、スマートカード・パーソナル化システム100はブロック1011にて、カード・オペレーティングシステム・データベース924からオペレーティングシステムに対する一連のプログラミング制御コマンドを獲得する。而して、各オペレーティングシステムに対するプログラミング制御コマンドは、チップメモリ内のファイルを生成かつアクセスし、チップメモリ内に配置されたファイル内にレコードを読み書きする如き機能に対するコマンドを、PIN（個人識別子番号）コードを認証すると共にチップ内に記憶された金額量を変更する取引きを制御するセキュリティコマンドと共に含んでいる。

ブロック1013にてスマートカード・パーソナル化システム100は、カード構造テンプレート・レコード内のパーソナル化用設備の識別子に対応する設備特性データを、パーソナル化用設備データベース926から獲得する。設備特性データに含まれるのは、パーソナル化用設備の作用を制御する一連のパーソナル化プログラミング制御コマンドである。カード・オペレーティングシステムと同様に、パーソナル化制御コマンドは設備の販売者に専有のものであるが、典型的には、ス

マートカードの管理、フォーマットおよび作成に関するコマンドを含んでいる。

スマートカード・パーソナル化システム100がスマートカードを定義するに必要なデータの全てを獲得したとき、それはカード発行者管理システム950からパーソナル化データレコード952を受ける用意ができる。ブロック1015にて各パーソナル化データレコード952が引渡されると、ブロック1017にて、スマートカード・パーソナル化システム100は、もし存在するならデータフォーマット・テンプレートを使用してパーソナル化データを内部フォーマットに変換すると共に、カード・アプリケーション・データおよびカード構造

テンプレートをを使用して、内部記述言語で書かれたコマンドスクリプト内の変数にパーソナル化データをマップする。変換処理およびマッピング処理は、以下に更に記述する。尚、内部記述言語の代わりにBasic、JavaもしくはCなどの標準的プログラミング言語を用いる代替の実施例は、本発明の範囲内である。

スマートカード・パーソナル化システム1019は、スマートカード発行プロセスの種々の構成要素に対してセキュリティ要件をチェックする。図11に示されたカード構造テンプレートの実施例においては、アプリケーションに対するセキュリティ要件はブロック1019においてカード構造テンプレート・レコード1100により指定される。もしセキュリティ要件があれば、ブロック1021にてスマートカード・パーソナル化システム100はセキュリティマネージャ940からセキュリティ・データおよび／または機能を獲得し、機能を内部スクリプトに加える。スマートカード・パーソナル化システム100の代替の実施例は、カード・オペレーティングシステムおよびパーソナル化用設備の識別子ならびにアプリケーション・プログラム識別子をセキュリティマネージャ940に引渡し、該セキュリティマネージャ940はセキュリティ・データベース942から適切なセキュリティ・データおよび／または機能を検索する。セキュリティ機能は典型的には、内部チップファイルに含まれたデータ、パーソナル化データ952、オペレーティングシステム・データベース924、カード・アプリケーション・データベース922を、チップ内に記憶されたアルゴリズムテーブルと組合せたデータを含む付加的ソースから、または、セキュリティマネージャ940などの外部セキュリティモジュールから、使用し

、これにより、図2に関して上述した安全キー認証、データの完全性、データ機密性、および他のセキュリティ処理を実現する。

内部コマンドスクリプトが一旦完了したなら、それは（もし存在するなら）カード・オペレーティングシステムおよびパーソナル化用設備に特有の専有プログラミング制御コマンドに変換され、パーソナル化データをスマートカードに転送せねばならない。この実施例においては、ブロック1025および1027にてスクリプト言語インタプリタにより変換が行われるが、これは、オペレーティングシステム・データベース924およびパーソナル化用設備データベース926から獲得された情報を用いて行われる。

ブロック1029において、スマートカード・オペレーティングシステム100はインタプリタされたスクリプトをパーソナル化用設備に引渡し、該パーソナル化用設備は、スマートカードの表面上および磁気ストライプおよびチップの夫々に適切なパーソナル化データをエンボス加工／印刷、コード化する為のプログラミング制御コマンドを実行する。前述の如く、カード発行者がアドオン式のスマートカードプログラミング装置を購入して自身の既存のパーソナル化用設備に取付けることを選択したのであれば、スマートカード・パーソナル化システム100の代替的实施例は、エンボス加工およびコード化用の制御コマンドをパーソナル化用設備930に導くと共に、チップ用の制御コマンドをスマートカード・プログラミング装置内のポストプロセッサ132に導く。

一枚のカードに対する発行プロセスが完了したとき、もし同一形式の付加的カードの発行が控えていれば、スマートカード・パーソナル化システム100は次のパーソナル化データレコードを獲得する（ブロック1033）。さもなければ、スマートカード・パーソナル化システムは別の形式のスマートカードの更なるバッチの発行が控えているか否かを判断し（ブロック1001）、且つ、カード発行者から新たなカード構造テンプレート・レコードを獲得することにより発

行プロセスを再開する。

以下の例は、図9および図10に示されたスマートカード・パーソナル化シス

テム100の実施例により実現される処理を更に記述すべきサンプルデータである。カード発行者管理システム950はスマートカード・パーソナル化システム100に対して発行プロセスの初期化を要求するが、これは、スマートカード・パーソナル化システム100に対して、カード構造テンプレート・レコード、アプリケーション・プログラム識別子、カード・オペレーティングシステム識別子、パーソナル化用設備の識別子、および選択的にデータフォーマット・テンプレート識別子またはデータフォーマット・テンプレート・レコードを送信することにより行われる。この例において、カード発行者管理システム950は、以下に示す各識別子を含むアプリケーション・リソース・テンプレート・レコードを引渡す。システム100は、上記に詳述すると共にサンプルのカード保持者データレコードに関して以下に更に詳述される処理のひとつを用いてデータフォーマット・テンプレートを獲得する。

アプリケーション・リソース・テンプレートのレコード

[A1]

DFT=CARD1. DFT

CAT=CARD1. CAT

C 識別子=CHIPX. C識別子

CPT=CARD1. CPT

SOURCE=A1

レコードの第1ステートメントは特定のアプリケーションに対する情報の開始をマークするものであり、この場合はアプリケーション“A1”である。次の4個のステートメントは、カード構造テンプレ

ート・レコード(DFT)、カード・アプリケーション・レコード(CAT)、カード・オペレーティングシステム・レコード(C識別子)およびパーソナル化用設備レコード(CPT)の夫々に対する識別子を定義している。最後のステートメントはカード発行者管理システム950により生成されたファイル名であり、カード保持者データレコードを含むものである。カード発行者管理システム950は、発行されるベ

きカードに対する単一の要求もしくは‘バッチ’要求のいずれかとしてカード保持者データを入力する。

システム100は識別子に対応するデータベースからレコードを検索する。システム100は次にカード構造テンプレートおよびデータフォーマット・テンプレートに含まれた情報を使用して内部“スクリプト”をセットアップするが、該スクリプトをシステム100は後の段階にて、各カード保持者に対するパーソナリゼーションデータを処理してカードを発行することをパーソナリゼーション設備に対して指示するカード・オペレーティングシステムおよびパーソナリゼーション設備レコード内に含まれた特定のコマンドにインタプリトする。

2個のサンプルカード保持者データレコード952が以下に示されている。

カード保持者データのレコード	
Smith, James	"12653683091245"0998"041052"mmmm
Anderson, Sue	"39485003984138"0297"110248"mmmm

これらのレコードにおいては、カード発行者により定義されたフォーマットは口座の名前（カード保持者の名前）を第1フィールドに置き、次に、口座番号、満了日、誕生日および医療データが続いている。

システム100はデータフォーマット・テンプレートを使用して、

カード保持者データ・レコード952の各々が処理されるときにそれをインタプリトする。システム100はまた、データフォーマット・テンプレートおよびカード・アプリケーション・レコード922を使用してデータ952を有効化し、適切なデータおよびフォーマットを確実なものとしている。上記に示されたサンプルのカード保持者レコードのフォーマットに対応するデータフォーマット・テンプレートの例は、以下の表の第1行に示されている。James Smithのパーソナリゼーションデータレコードが表中に含まれて、データフォーマット・テンプレートとカード保持者データレコードの各フィールドとの間の対応を示している。データフォーマット・テンプレートはカード保持者レコードの各フィールドを内部ラベル%1、%2などで象徴しているが、これは、システム100内で使用される内部順序に対応してい

る。

データフォーマット・テンプレートのレコード					
	%1		%2		%3 %4 %5
Smith, James ^ 12653683091245 ^ 0998 ^ 041052 ^ mmmmm					

上記に示した例は最も単純な場合であり、カード保持者データ・レコード952の各フィールドはスマートカード・パーソナリ化システム100により使用される内部順序で配置されている。この1対1対応は、システム100がカード保持者データフィールドを変換する必要が無い、ということ意味している。斯かる場合、データフォーマット・テンプレート・レコードは不要である。従って、更なる代替の実施例において、カード発行者はデータフォーマット識別子をスマートカード・パーソナリ化システム100に対して引渡さず、代わりに、フラグなどのインディケータを引渡すが、これはシステム100に対し、カード保持者データフィールドが内部フィールド順

と1対1対応であることからデータフォーマット・テンプレートが不要であることを告げるものである。システム100は変換段階をバイパスすることにより、インディケータに作用する。

次に示される更に複雑な例は、カード保持者データ・レコード952の各フィールドおよび各フィールド内のデータが内部システム順に対して同順となっていない例である。この場合、変換が必要である。

発行者フォーマットによるカード保持者のデータ	
1234567891245 James Smith 0998 041052 mmmmm	
内部フォーマットに翻訳されたカード保持者データ	
Smith, James "12653683091245"0998"041052"mmmmmm	

システム100はデータフォーマット・テンプレートを用いてデータフィールドを上記に示した内部順序に変換する。この変換は、データフィールドの物理的配置に帰着しても良く、または、カード保持者データレコードからのフィールド

がシステム100により参照される毎にデータフォーマット・テンプレートがキーとして呼出されるという論理再配置であっても良い。当業者であれば、種々の配置構成のカード保持者データを変換すべく設計された種々のデータフォーマット・テンプレートは明らかであろう、と言うのも、この例を示すべく上記で用いられた単純な表に対するフィールドの同等性または一連の解析指示または他のメカニズムの置換えだろうからである。

カード構造テンプレート・レコードは、カード上のチップの構造を記述する。以下に示したサンプルにおいては、\$MFエントリはルートディレクトリ(3F00)、\$DFエントリは医療アプリケーション(5F20)および会計アプリケーション(5F10)を定義している。各ディレ

クトリ内においては、アプリケーションに特有のファイルが\$EFエントリにより定義されているが、これは、口座名を含む6F00および口座番号を含む6F10などである。全てのファイル記述データはカード構造テンプレート内に在り、且つ、スマートカード発行プロセスの間の種々の時点で参照される。

カード枠組テンプレートのレコード

```
$CHIP=3102, MEM=8192, SIZE=N10

$MF PATH=x3F00, TAG=ROOT, TITLE= 'Root Directory' ,
                                SIZE=D7194

$DF PATH=x3F005F10, TAG=ACCT, TITLE= 'Acct Data' ,
                                SIZE=D2048

$DF PATH=x3F005F20, TAG=MED, TITLE= 'Medial' , SIZE=D1024

$BF PATH=x3F003100, TAG=ICC 識別子, TITLE= 'Issuer
                                識別子' , FORMAT=T, SIZE=D10

$BF PATH=x3F005F205E00, TAG=MED1, TITLE= 'Medical
                                profile' , FORMAT=T, SIZE=D80

$EF PATH=x3F005F106F00, TAG=NAME, TITLE= 'Acct
                                Name' , FORMAT=T, SIZE=A30

$EF PATH=x3F005F106F10, TAG=ACCT識別子, TITLE= 'Account
                                No.' , FORMAT=T, SIZE=N14

$EF PATH=x3F005F106F20, TAG=EXPIRE, TITLE= 'Expire
                                Date' , FORMAT=T, SIZE=N4

$EF PATH=x3F005F106F30, TAG=BIRTH, TITLE= 'Account Holder
                                Birthdate' , FORMAT=T, SIZE=N6
```

カード・アプリケーション・レコード922はカード保持者データ952をアプリケーションにより使用されるデータフィールドに“マ

ップ”する。以下に示されるサンプルのカード・アプリケーション・レコード922は、スマートカード・パーソナリ化システム100により処理されるシーケンスで配置されたデータエントリを有している。

カード・アプリケーションのレコード

\$VL ICC 識別子 VALUE=1234509876
\$VL MEDI%5, TYPE=A
\$VL NAME%1, TYPE=A
\$VL ACCT識別子%2, TYPE=N
\$VL EXPIRE%3, TYPE=N
\$VL BIRTH%4, TYPE=N
\$VL FMTACCT%2(1-4)-%2(5-9)-%2(10-14)

ICC識別子エントリはチップ識別子を含む。FMTACCTを除き、残りのエントリの各々は、カード保持者データ・レコード952内のフィールドへの“タグ”をマップするが、これは（上記に示したデータフォーマット・テンプレート中に定義された）情報を含むと共にフィールド内のデータの形式を指定するものである。従って、MEDIタグはカード保持者データ・レコード952の第5フィールドを示すと共にデータはアルファベットである。FMTACCTエントリはカード保持者データ・レコード952の第2フィールド、即ち口座番号、を複数の部分に細分し各部分間にハイフンを挿入している。

カード・オペレーティングシステム・レコード924は、カード上のチップをプログラムするに必要なプログラミング制御コマンドを含んでいる。以下に示されるサンプルのカード・オペレーティングシステムのプログラミング制御コマンドはISO指示番号7816-4から導かれたものであり、任意の特定のカード・オペレーティングシス

テムの内部専有コマンドではない。

カード・オペレーティングシステムのレコード

SELECT A0A4000002%F

WRITE A0D0%0%L%D

READ A0B0%0%L%D

RESET VALUE=xFF

上記例のレコードにおける各エントリはタグを含み、これにはカード・オペレーティングシステム本来の言語における対応コマンドが続く。可変パラメータフィールドはその後に文字が続く“%”により示され、個々のカードが処理されるときに適切なカード保持者データにより埋められる。

パーソナル化用設備レコード926は、特定のパーソナル化用設備セットで完全なカードを発行する為に必要な実際のシーケンスおよびステップを定義する命令などの、パーソナル化用設備特性データを含んでいる。この例で使用されたサンプル命令は現実のものではなく、何らかの特定のパーソナル化用設備に対する内部専有命令を表すものではない。

パーソナル化用設備のレコード

\$EMBOSS

#EMB#%FMTACCT%“%NAME%

\$ENCODE

#ENC#%%%ACCT識別子%“%NAME%

\$IC

\#@#

@ICC識別子

```
WRITE ICC 識別子
@NAME
SELECT ACCT
SELECT NAME
WRITE NAME
@ACCT 識別子
SELECT ACCT 識別子
WRITE ACCT識別子
@EXPIRE
SELECT EXPIRE
WRITE EXPIRE
```

\$PR

各カードが発行されるとき、上記に示されたパーソナル化用設備特性データは、“\$”が先頭に付されたエントリにより定義された4つの段階で順番に処理される。而して、カード・アプリケーション・レコード922は、各命令において可変パラメータフィールドの値を決定すべく使用される。

\$EMBOSS命令は、これに引続くデータをカードにエンボス加工すべきことをパーソナル化用設備に通知する、制御シーケンス#EMB#により始まる単一データストリームである。命令の各データフィールドは一对の%記号で挟まれている。この場合、第1のデータフィールドはFMTACCTであり、即ち、カード・アプリケーション・レコード922で定義されたフォーマット口座フィールドである。システム100はFMTACCTエントリに関してカード・アプリケーション・レコード922をサーチし、第1のサンプルカード保持者レコード952の第2データフィールドからストリング“1265-36830-91245”を生成する。次のフィールドであるNAMEはカード保持者レコード952の

第1データフィールドから取り出される。従って、第1サンプルのカード保持者レコード952に対するエンボス加工命令は、#EMB#%1265-36830-91245%%Smith, Jam

es%となる。

\$ENCODE命令はシステム100に対し、エンボス加工命令と同様の手法でカードの磁気ストライプにカード保持者データをコード化する処理を行わせる。コマンド内には、次のIATA(国際民間航空輸送協会)およびISO基準に従う付加的な制御キャラクタが挿入される。最終的な命令は、#ENC###%12653683091245%Smith, James%である。

\$ICコマンドは、チップのメモリ内に記憶されるべき情報を指定する。カード・オペレーティングシステム・レコード924は、パーソナル化用設備レコード内の命令を、オペレーティングシステム用のプログラミング制御コマンドに変換すべく使用される。制御シーケンス即ち#@#は、パーソナル化用設備に対し、引続くデータがチップデータであることを通知するものである。記憶されるべき最初のフィールドは、チップ識別子すなわちICCIDである。システム100は、パーソナル化用設備レコード926内のWRITEタグを、カード・オペレーティングシステム・レコード924内のWRITEタグにより指定されたコマンドに従ってインタプリトする。チップ識別子エントリに対してアプリケーション・レコード922で指定されたオフセット値は無いことから、%0変数パラメータフィールドには既定値“0000”がロードされる。%L変数パラメータフィールドには、カード構造テンプレート内の\$CIHPエントリ内のSIZEフィールドの値である“10”即ち16進数“0A”がセットされる。%D変数パラメータフィールドには、ICCIDの値である“1234509876”がセットされる。最終的なコマンドはA0D000000A1234509876である。

次のコマンドは、カード・オペレーティングシステムに対し、チップ上の口座ディレクトリ内の口座名ファイルにカード保持者氏名

を記憶させる。システム100はSELECT ACCTコマンドを対応するカード・オペレーティングシステム・コマンドに変換する。システム100はカード・オペレーティングシステム・レコード924内のSELECTエントリ、カード構造テンプレート・レコード内のACCTエントリを発見すると共に、ACCTエントリで定義された口座ディレクトリに対して指定されたディレクトリパス即ち“5F10”で、SELECTエントリで定義されたコマンド内の%F変数パラメータフィールドを置換える。結果的なコ

マンドはA0A40000025F10である。同様に、SELECT NAMEコマンドはシステム100に対し、口座名ファイル“6F00”で%F変数パラメータフィールドを置換えさせる。結果的なコマンドはA0A40000026F00である。この繋がり最終コマンドはWRITEコマンドである。システム100はWRITEコマンドをインタプリトするが、これは、%0を既定オフセット“0000”で置換え、%Lを、カード構造テンプレート・レコード内のNAMEエントリにより定義されたSIZEフィールドの値“30”即ち16進数“1E”で置換え、且つ、%Dを、第1 サンプルカード保持者レコード952に対するカード保持者氏名“Smith, James”で置換えることを行い、これにより、コマンドA0D000001ESmith, James~~~~~を生成するが、各“~”は氏名を30文字まで引き伸ばすべく挿入された継続スペースを示している。

システム100はパーソナリ化用設備レコード926内の残りのコマンドを同様に処理し、第1 サンプルカード保持者レコード952に対してカードを発行する為のコマンドを含むデータの連続的ストリングを生成する：

```
# \#@#A0D000000A123459876A0A40000025F10A0A40000026F
00A0D000001ESmith, James ~~~~~
~A0A40000
```

026F10A0A4000002E12653683091245A0A40000026F2040998,
\$PRコマンドはシステム100に対し、コマンドデータ・ストリームをパーソナリ化用設備に送信させる。

図11、図12および図13に示されたデータ・レイアウト、および、上記のサンプルに関して上述したサンプルデータは、スマートカード・パーソナリ化システム100の種々の実施例の機能を示すべく用いられた例にすぎない。当業者であれば、レイアウトおよびデータはそれらが使用される環境により必然的に定義されることは明らかであろう。

当業者には明らかな様に、スマートカード・パーソナリ化システム100は、システムの各機能が添付図面中に示されたものと異なるモジュールにより実現されるソフトウェアプログラムの代替的实施例を包含するものである。また、本発明

の精神もしくは範囲から逸脱すること無く、システム100はデータをシリアルに
もしくはパラレルに、または、両者を組合せて処理しても良い。ソフトウェアプ
ログラムは広く入手し得る幾つかのプログラミング言語のひとつで書かれて良く
、且つ、各モジュールは、選択された言語に依り、サブルーチン、サブシステム
もしくはオブジェクトとしてコード化され得る。同様に、システム100により使
用されたデータはデータベース内に実現された論理レコードとして記述されかつ
示されたが、本発明は記述されたデータレコードに限定されるものでなく、何ら
かの特定の形式のデータ管理システムを意味するものでも無い。また、Oracle、
Sybase、InformixもしくはMicrosoftなどの販売者からのリレーショナル・デー
タベースは、集中化されもしくは分散されるかに関わり無く、システム内の基礎
データを管理する上で必要なインフラストラクチャを提供するが、本発明の範囲
を越えることなく、例えばインデクス付きフラットファイル等の他の機構のデー

タ構造で置換えても良い。

更に、ハードウェア、ファームウェア、もしくはハードウェアとソフトウェア
との両者の組合せで上記システムを実現する本発明の代替的实施例、並びに、モ
ジュールおよび／またはデータを別の手法で配分することは、当業者には自明で
ありかつ本発明の範囲内である。

上記説明は例示的なものであり限定的なものではないことは理解されよう。当業
者であれば、上記記載に鑑みて他の多くの実施例が明らかであろう。故に、本発
明の範囲は、添付の請求の範囲の権利対象となる均等物の最大範囲と共に、添付
の請求の範囲を参照して定められねばならない。

【図1A】

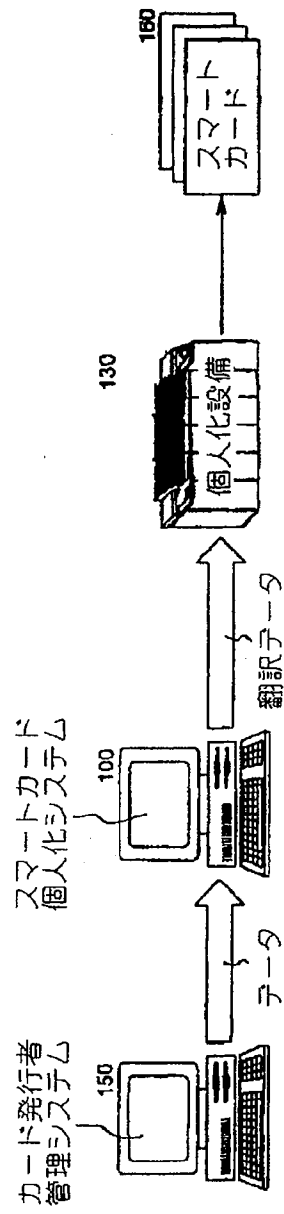


Figure 1A

【図1】

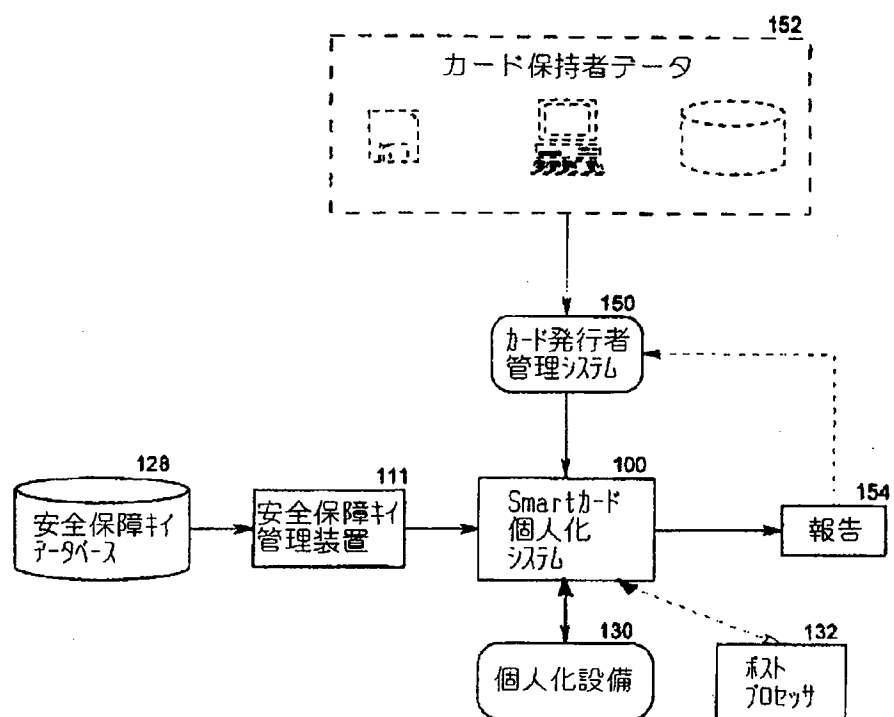


Figure 1B

【図1】

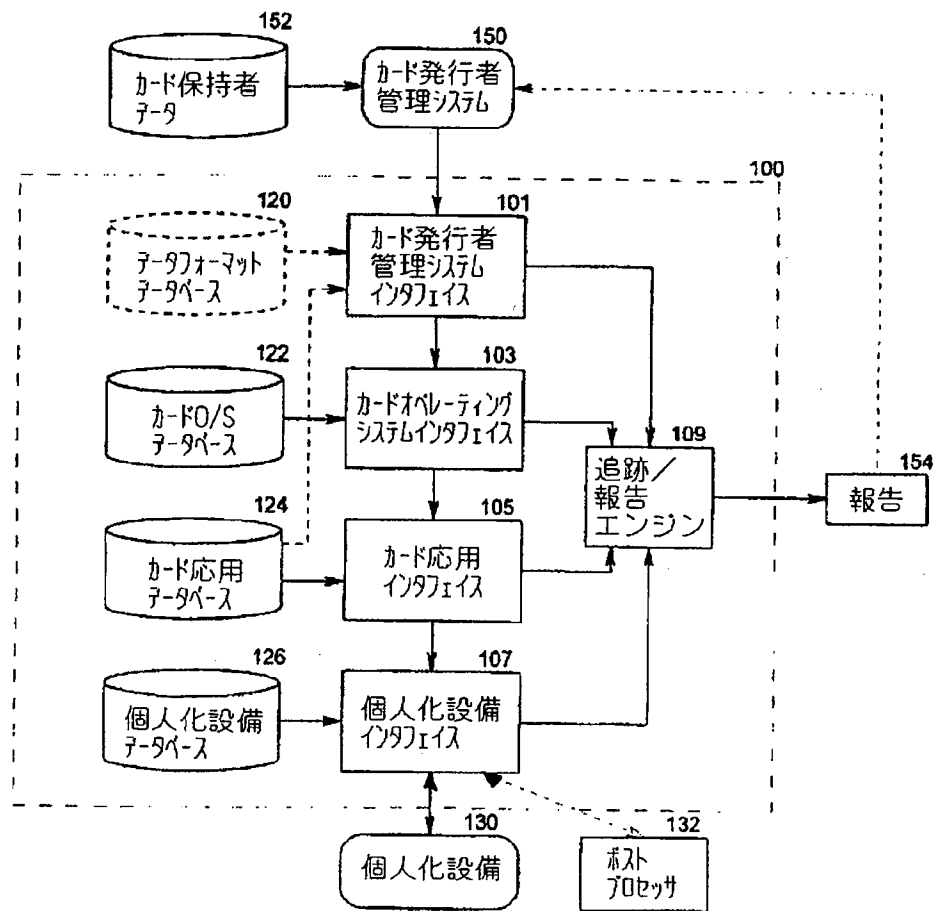


Figure 1C

【図 2】

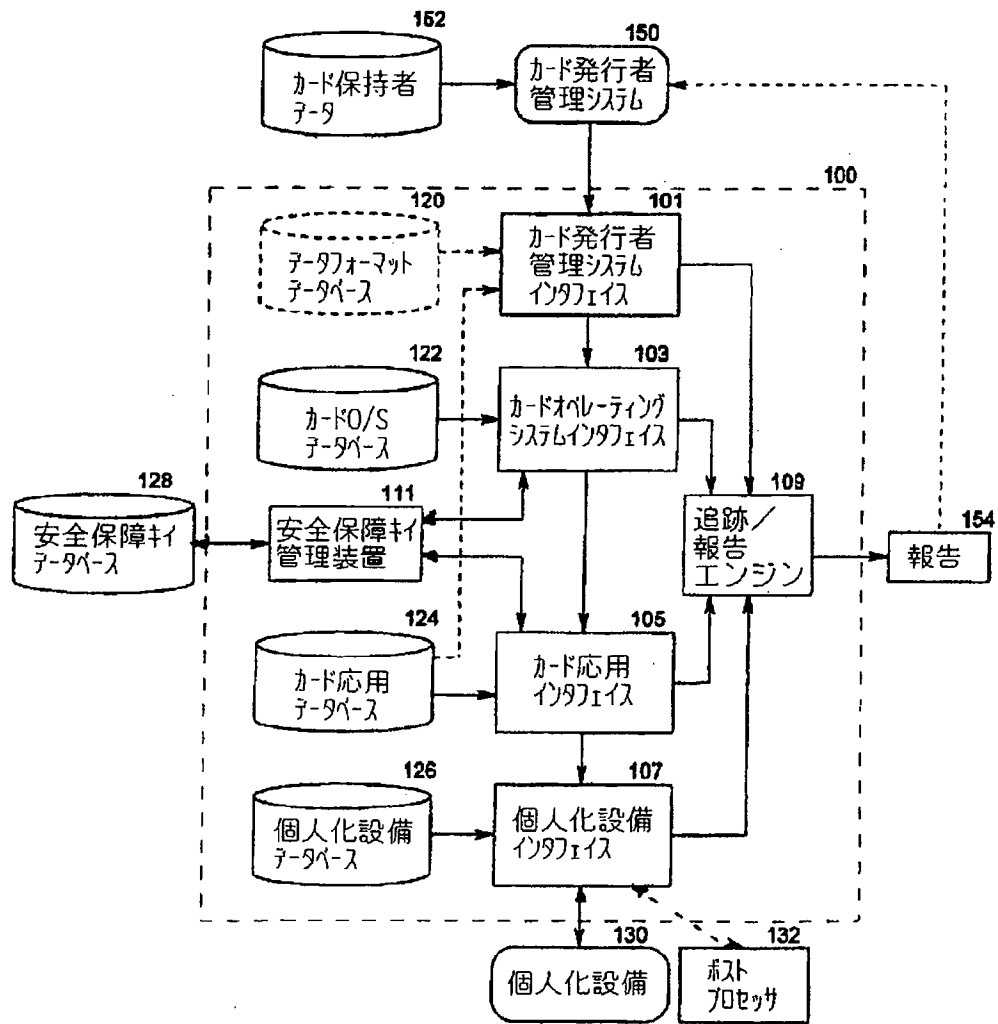


Figure 2

【図3】

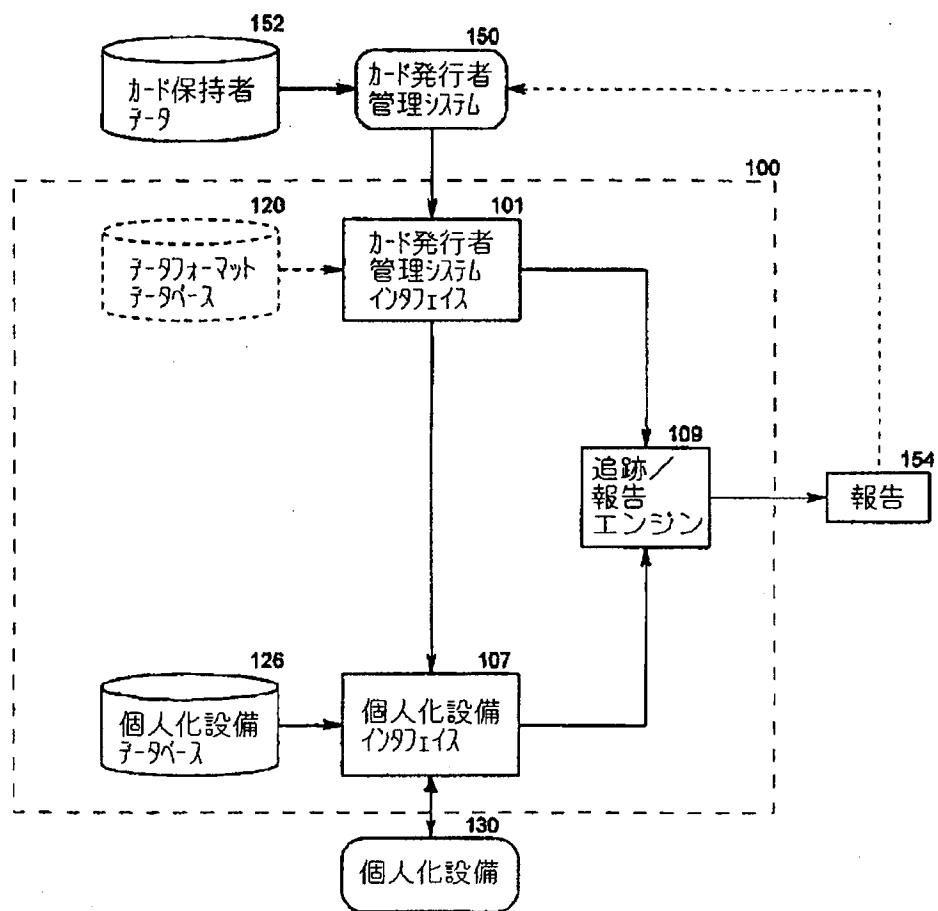


Figure 3

【図4】

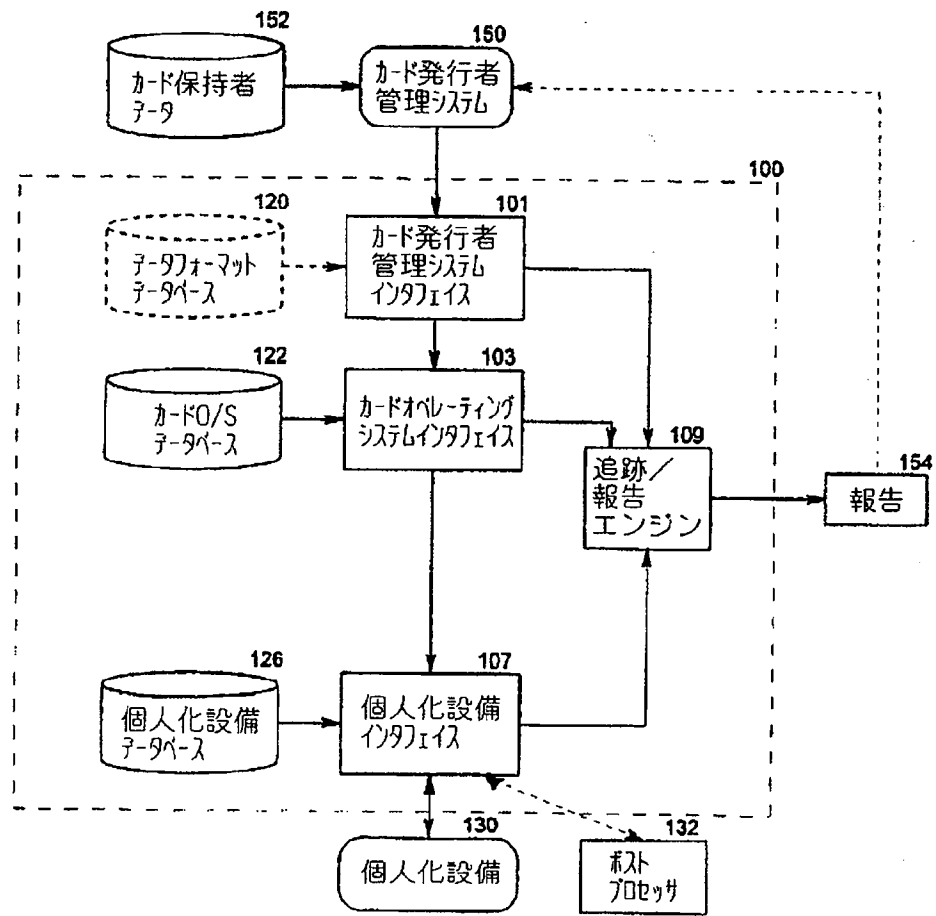


Figure 4

【図5】

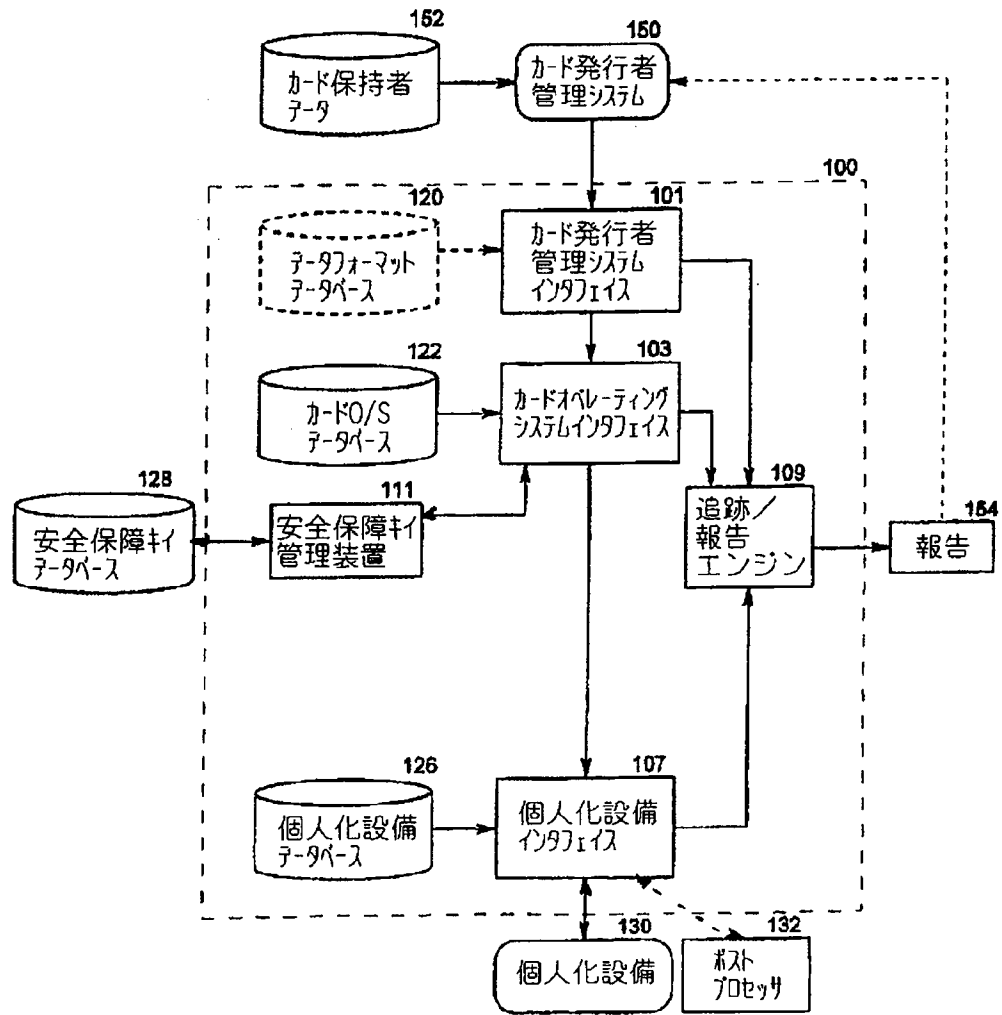


Figure 5

【図6】

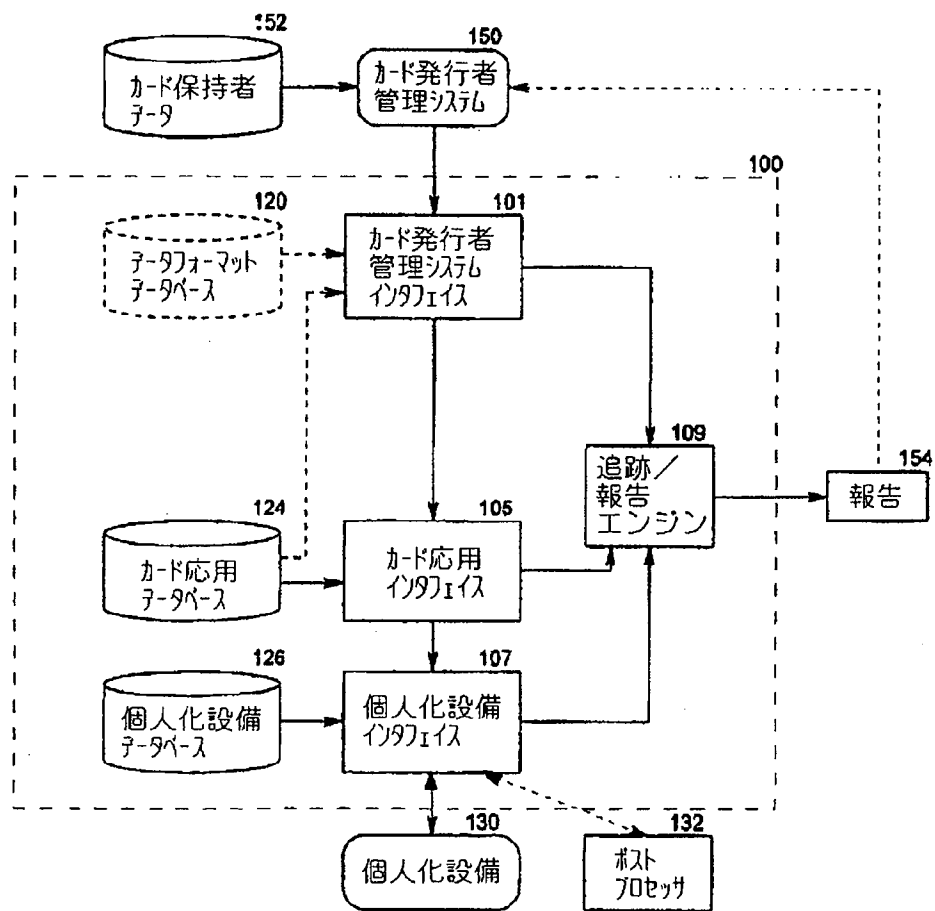


Figure 6

【図 7】

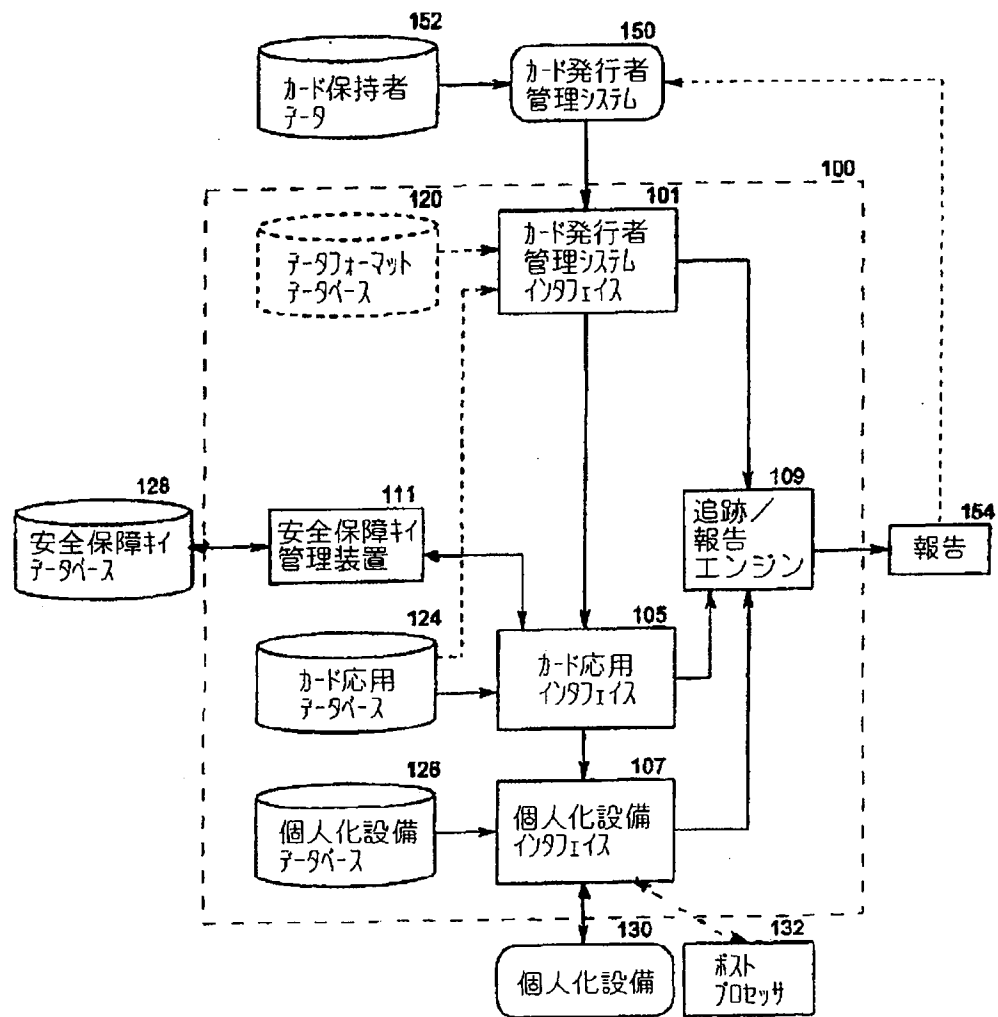


Figure 7

【図8】

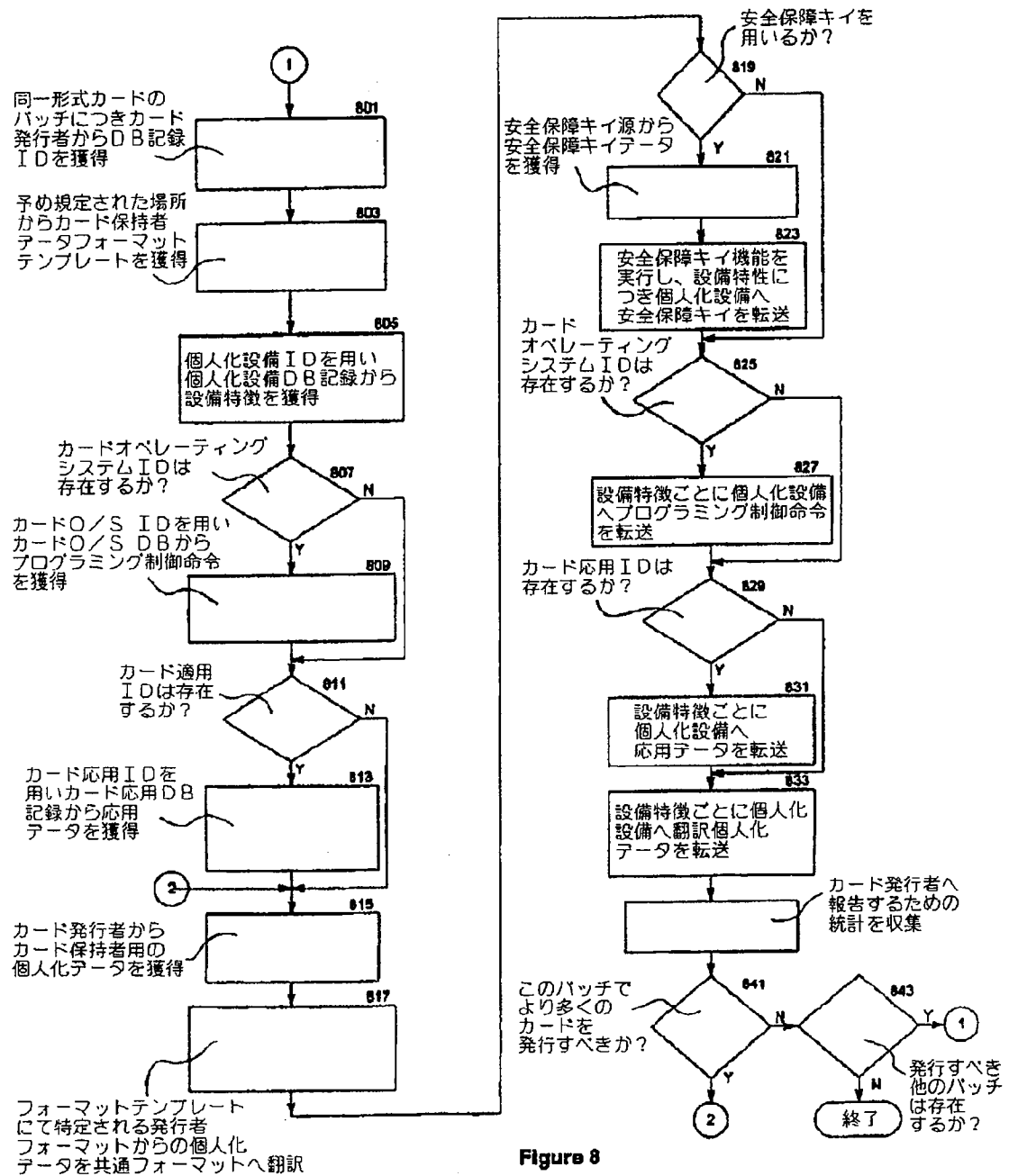


Figure 8

【図9】

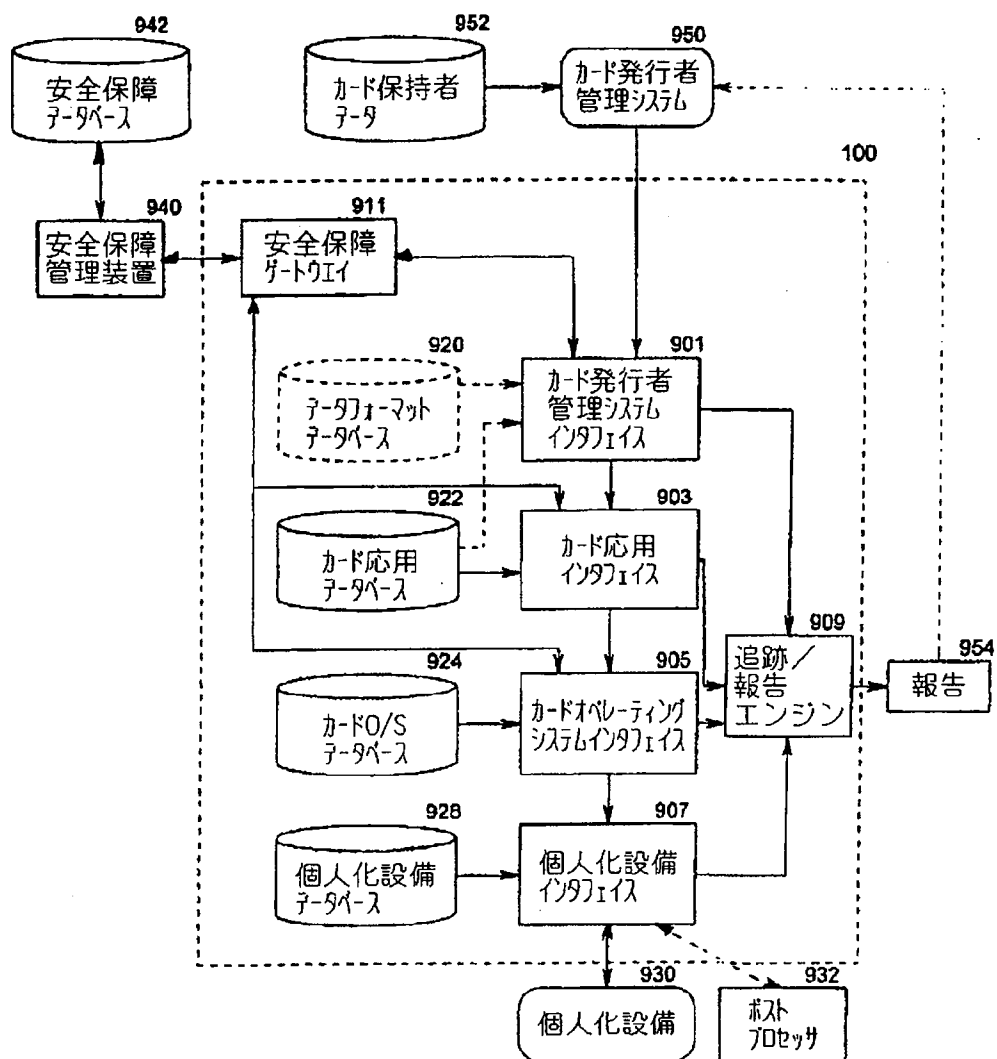


Figure 9

【図10】

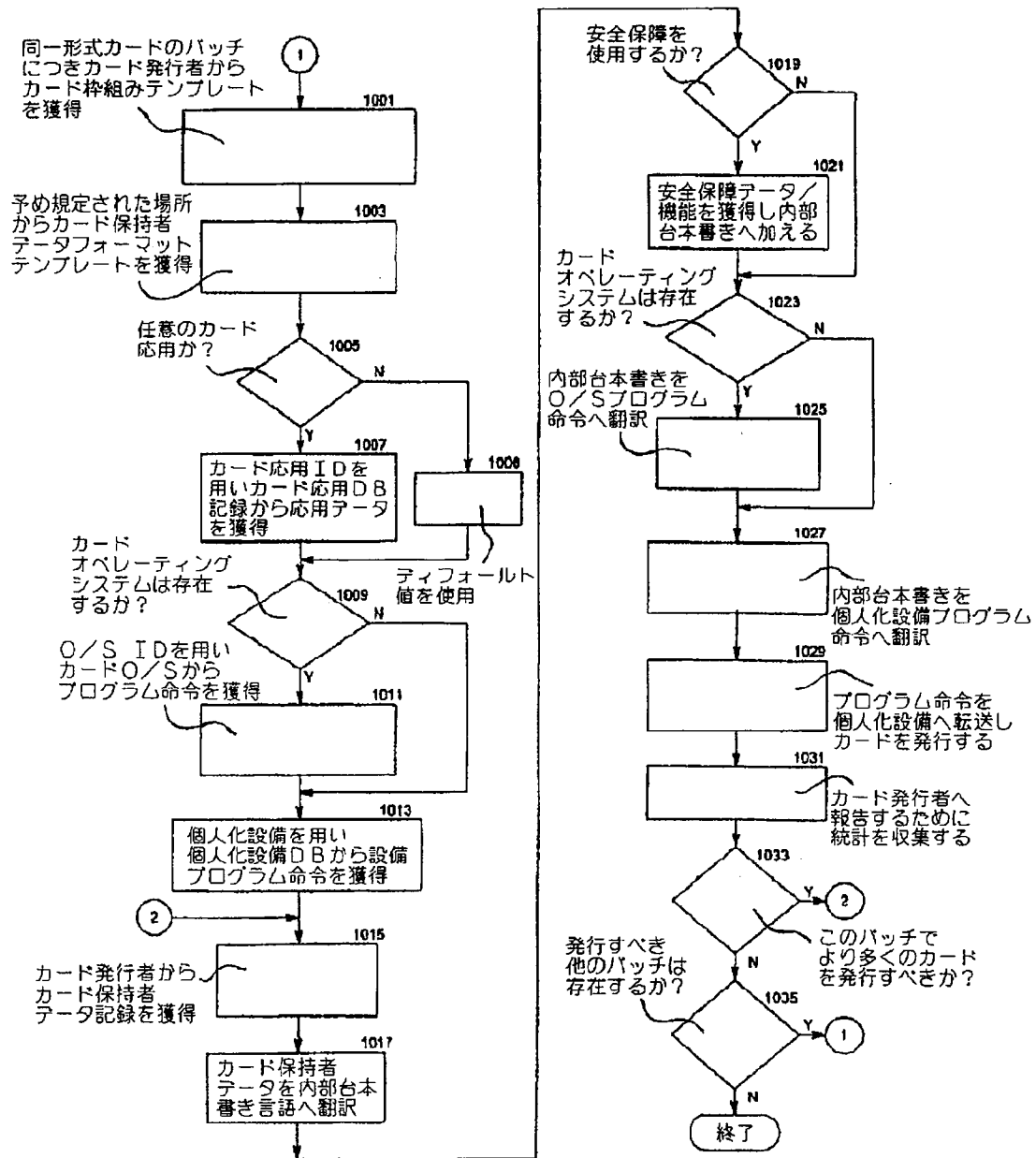


Figure 10

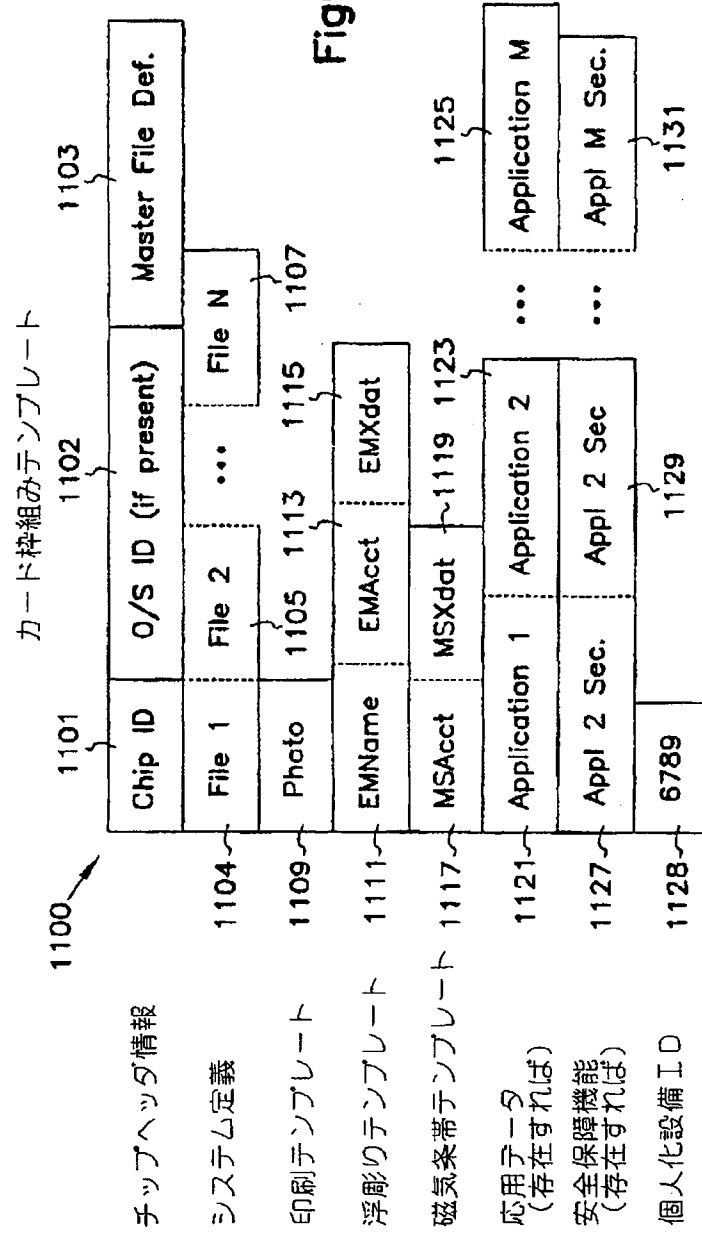


Figure 11

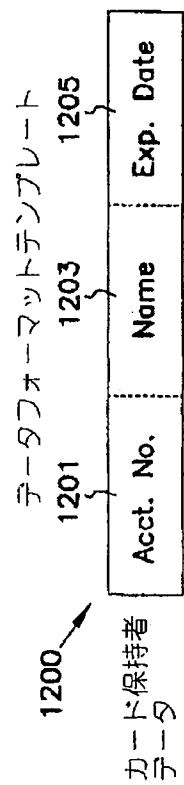


Figure 12

【図13】

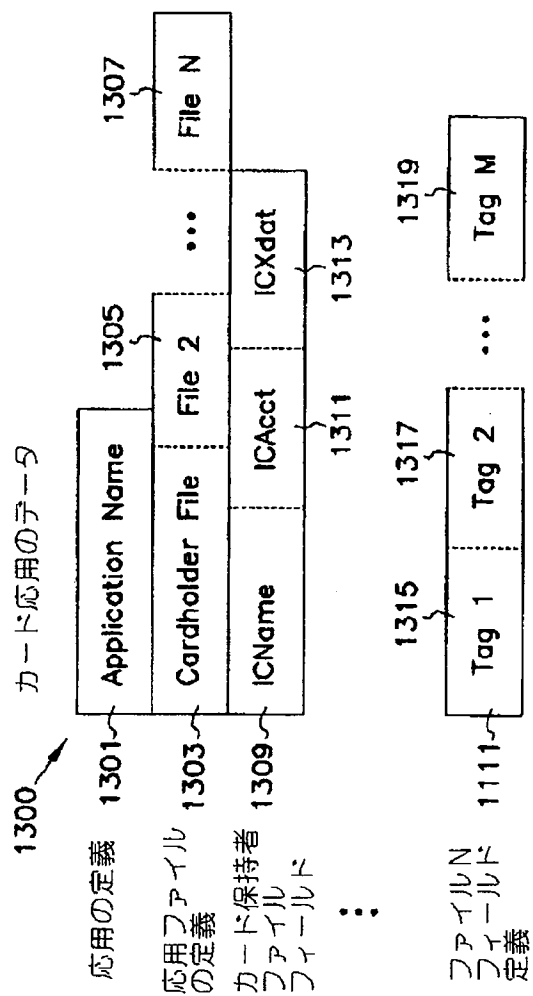


Figure 13

【図 14】

報告項目の例

<p>カードのストック 部分の番号 アカウント名称 部分の記述 プラスチック マイクロコントローラ 磁気ストライプ 持合わせの量 記録装置の水準 プロジェクトされる次位の記録装置の日付け／量 在庫補充のデータ 受理したロット番号 売り主 受理した日付け 量 良品／不合格品 在庫使用のデータ 作業の番号 日付け チェックアウトされた量 チェックバックインされた量</p>	<p><u>材料の状態</u> フォームのストック 部分の番号 アカウント名称 部分の記述 持合わせの量 記録装置の水準 プロジェクトされる次位の記録装置の日付け／量 在庫補充のデータ 受理したロット番号 売り主 受理した日付け 量 良品／不合格品 在庫使用のデータ 作業の番号 日付け チェックアウトされた量 チェックバックインされた量</p>
<p><u>ソフトウェア形態</u> 顧客のライブラリ インタフェースライブラリの成分 応用のライブラリ キイのカード 応用データライブラリの成分 カードO/Sのライブラリ バッチのカード カードO/Sライブラリの成分 個人化設備のライブラリ 支持される個人化装置</p>	<p><u>産出状態</u> 機械のバッチ バッチ起源のデータ 管理 ベアレントの作業 操作者 日付け／時間 顧客 カードの形式 応用 日付け 安全保障の要求 静的 動的 オペレーティングシステム 動的安全保障の要求 プラスチックカード形式（部分の番号） カードの数 個人化装置 チップ個人化装置 カード個人化装置 産出 個人化されたカード カードの誤り 誤りの形式 カードの総計</p>

Figure 14

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/06204

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : G06K 19/06; G06F 11/00

US CL : 395/186

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 395/186; 235/ 375, 380; 395/241

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS, CAS ONLINE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,442,165 A (ATSUMI et al.) 15 August 1995, see the abstract, figure 2, and col. 4, lines 7-64	1-31
Y	US 4,866,259 A (BONNEMOY) 12 September 1989, see the abstract, figure 1	1-31
Y, P	US 5,578,808 A (TAYLOR) 26 November 1996, see the abstract, figure 3	1-31

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:	* T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
* A document defining the general state of the art which is not considered to be of particular relevance	* X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
* E earlier document published on or after the international filing date	* Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
* L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	* & document member of the same patent family
* O document referring to an oral disclosure, use, exhibition or other means	
* P document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

28 JUNE 1997

Date of mailing of the international search report

21 AUG 1997

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized Officer

ALBERT DECADY

Telephone No. (703) 308-3900

Form PCT/ISA/210 (second sheet) (July 1992)*

フロントページの続き

(81)指定国 EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(GH, KE, LS, MW, SD, SZ, UG), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, YU